NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AVIATION SECURITY: BIOMETRIC TECHNOLOGY AND RISK BASED SECURITY AVIATION PASSENGER SCREENING PROGRAM

by

Curt S. Cooper

December 2012

Thesis Co-Advisors: Lauren Fernandez
Kathleen Kiernan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2012	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE AVIATION SECURITY; BIOMETRIC TECHNOLOGY AND RISK BASED SECURITY AVIATION PASSENGER SCREENING PROGRAM	5. FUNDING NUMBERS
6. AUTHOR(S) Curt S. Cooper	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	A

13. ABSTRACT (maximum 200 words)

Since 9/11, the Transportation Security Administration (TSA) has struggled to maintain a balance between providing a secure world-class aviation passenger-screening program (APSP) while providing efficiency, convenience and security for the traveling public and the airline industry. For years the TSA has applied resources and procedures uniformly to all passengers during aviation passenger screening. It is mainly a "one size fits all " screening where all passengers are treated as equal risk, which has exponentially increased resources, procedures and equipment required to do aviation passenger screening,

Recently, the Transportation Security Administration has sought to find a better way to conduct aviation passenger screening and is transitioning to Risk Based Security (RBS). The RBS initiatives have greatly improved the aviation passenger screening experience while increasing the efficiency of checkpoint screening by shortening the amount of wait times. Furthermore, it has allowed resources to be applied to high-risk individuals and lessen the burden of passenger screening on low-risk individuals. This has freed up resources reduced procedures while simultaneously increasing the efficiency of the checkpoint.

The research here provides options on how to better enable current RBS initiatives by incorporating biometric technology into the aviation passenger-screening program. This research has reviewed other government programs that have incorporated biometrics into their procedures to improve the efficiency and reliability by using biometrically enhanced security measures. Through the application or modification of these biometrically enhanced security programs of other agencies, the TSA could standardize and incorporate biometrics into the RBS APSP allowing for authentication of both identity verification and identification. This research will explore how to incorporate biometrics into the current Risk-Based Security Aviation Passenger Screening Program.

14. SUBJECT TERMS Biometrics, Aviation Security, Risk-Based Security, Aviation Passenger Screening Program, Biometrically Enhanced Security Programs, Transportation Security Administration	15. NUMBER OF PAGES 129
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AVIATION SECURITY: BIOMETRIC TECHNOLOGY AND RISK BASED SECURITY AVIATION PASSENGER SCREENING PROGRAM

Curt S. Cooper
Department of Homeland Security
Transportation Security Administration
B.S., Niagara University, New York, 1988
M.P.A. Troy University, Alabama 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2012**

Author: Curt S. Cooper

Approved by: Lauren Fernandez
Thesis Co-Advisor

Kathleen Kiernan
Thesis Co-Advisor

Dan Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Since 9/11, the Transportation Security Administration (TSA) has struggled to maintain a balance between providing a secure world-class aviation passenger-screening program (APSP) while providing efficiency, convenience and security for the traveling public and the airline industry. For years the TSA has applied resources and procedures uniformly to all passengers during aviation passenger screening. It is mainly a “one size fits all “ screening where all passengers are treated as equal risk, which has exponentially increased resources, procedures and equipment required to do aviation passenger screening,

Recently, the Transportation Security Administration has sought to find a better way to conduct aviation passenger screening and is transitioning to Risk Based Security (RBS). The RBS initiatives have greatly improved the aviation passenger screening experience while increasing the efficiency of checkpoint screening by shortening the amount of wait times. Furthermore, it has allowed resources to be applied to high-risk individuals and lessen the burden of passenger screening on low-risk individuals. This has freed up resources reduced procedures while simultaneously increasing the efficiency of the checkpoint.

The research here provides options on how to better enable current RBS initiatives by incorporating biometric technology into the aviation passenger-screening program. This research has reviewed other government programs that have incorporated biometrics into their procedures to improve the efficiency and reliability by using biometrically enhanced security measures. Through the application or modification of these biometrically enhanced security programs of other agencies, the TSA could standardize and incorporate biometrics into the RBS APSP allowing for authentication of both identity verification and identification. This research will explore how to incorporate biometrics into the current Risk-Based Security Aviation Passenger Screening Program.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABC	Automated Border Clearance
ABIS	Automated Biometric Identification System
ACLU	American Civil Liberties Union
AFGE	American Federation of Government Employees
AIT	Advanced Imaging Technology
APSP	Aviation Passenger-Screening Program
ASM	Available Seat Miles
ATR	Automatic Target Recognition
ATSA	Aviation and Transportation Security Act
BDO	Behavior Detection Officer
BIMA	Biometric Identity Management Agency
CAC	Common Access Card
CASS	Cockpit Access Security System
CBP	Customs and Border Protection
CJIS	Criminal Justice Information Services
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	Department of State
DNA	Deoxyribonucleic Acid
DOB	Date Of Birth
ETD	Explosive Trace Detection
FBI	Federal Bureau of Investigation
GAO	Government Accountability Office

HSPD	Homeland Security Presidential Directive
IAFIS	Automated Fingerprint Identification System
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
KCM	Known Crew Member
KST	Known Suspected Terrorist
LEO	Law Enforcement Officer
MTSA	Maritime Transportation Security Act
NGI	Next Generation Identification
NSPD	National Security Presidential Directive
NSTC	National Science and Technology Council
POE	Point Of Entry
RBS	Risk-Based Security
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
SFPD	Secure Flight Passenger Data
SORN	System Of Records Notice
SPOT	Screening of Passengers by Observation Techniques
SSN	Social Security Number
TSA	Transportation Security Administration
TDC	Travel Document Checker
TSO	Transportation Security Officer
TWIC	Transportation Worker Identification Card
USCG	United States Coast Guard
WTMD	Walk Through Metal Detector

ACKNOWLEDGMENTS

Through life's journey there are many people who will recognize you for the potential you have and provide you the opportunity to reach out for success. This endeavor, as life is no different. There are many individuals who provided me the guidance, mentorship and counsel needed to complete the program and this thesis. I dedicate this thesis to them for without their support and belief in my potential this could not have been possible. Those I owe the most to are my family for the countless hours of sacrifice of "our" time. To Conor, Carson and Cadence, now that this journey is complete I will make it up to you. To my wife Rebecca, who has been the lynch pin in this journey; you have been my counsel, my typist, my editor, my researcher (nice having a wife who is a librarian), but most importantly you are my best friend and confidant. This thesis would not have been possible without you; the countless early mornings and late nights reviewing draft after draft. Rebecca, I love you. Thank you.

Next, to the faculty and staff of the Center for Homeland Defense and Security (CHDS), from the operational support to the professors, your dedication and unwavering support are second to none and have made this experience truly enriching and unforgettable. Particularly I would like to thank my advisors Dr. Laura Fernandez and Dr. Kathleen Kiernan for their exceptional guidance, direction and editing. I would also like to mention Dr. Richard Bergin whose classroom instruction gave me the idea of using biometrics.

I would like to thank my organization, TSA for sponsoring me in this world-class program. I would like to personally thank Mr. Ken Kasprisin, Mr. Tom Connors and Mr. Drew Rhoades without whom this 18-month journey could not have been possible since I had to balance the demands of work, my family and my community with the demands of this program. Their willingness to absorb my two-week absences to attend the in-residence classes in this program is greatly appreciated.

Finally, I would like to thank the thousands of TSA workers who work day in and day out unwaveringly to provide world-class aviation passenger security. I would especially like to thank the workers at Minneapolis/St Paul International Airport. I truly believe they are second to none and lead the way in the country. It is my wish that this thesis will improve the nature and procedures of the aviation passenger screening program easing the burden and changing the dynamics and effectiveness of aviation passenger screening.

I. INTRODUCTION

"We do use a one-size-fits-all approach, which I don't think is either efficient or beneficial for the traveling public or for security."

TSA Administrator Pistole, Congressional Testimony, 10 February 2011

A. BACKGROUND

In November 2001, Congress enacted the Aviation and Transportation Security Act (ATSA) of 2001. This was the essential legislation that created the Transportation Security Administration (TSA). It was perhaps best known for "federalizing" airport security by creating a large federal workforce of passenger and baggage screeners to replace the private contract screeners previously employed by airlines, to staff passenger screening checkpoints at airport concourses. (Poole, 2006, p.1) Since the federalization of passenger screening, every day in the United States, approximately 2 million air travelers travel throughout the country and are subjected to a "one-size-fits-all" screening system. The TSA's Aviation Passenger Screening Program (APSP) process uses massive amounts of federal resources, creates frustration amongst the traveling public with long lines and wait times, impacts the airline industry and U.S. economy, and is not the most effective or efficient way to conduct passenger screening. The aviation passenger-screening program mainly applies an "equal risk" model to all passengers and does not differentiate between suspected terrorists or the 1 million-mile frequent flier business traveler. In the summer of 2011,TSA Administrator John Pistole introduced Risk-Based Security (RBS) to the TSA. The Risk-Based Security model uses information gained during pre-screening, along with thorough observation and interaction with passengers to determine the proper level of screening that matches the passenger's risk assessment. The RBS model will allow the TSA to re-focus some resources on higher risk or unknown risk travelers thereby increasing security efficiency and

effectiveness. (Transportation Security Administration n.d., p. 6) There is an even better way to improve the new Risk-Based Security aviation passenger-screening program.

The current passenger-screening program method has not fully adopted the National Security Presidential Directives and Homeland Security Presidential Directives (HSPD-59/HSPD24). The HSPDs call for the use of biometrics for identification and screening to enhance national security. (The White House, 2008, p1.) Congressional reports show the TSA and other governmental agencies have failed to adopt fully effective strategies, policies and technology that meet the HSPDs, while at the same time ignore longstanding Congressional statues to establish biometric credentialing standards for passenger screening (U.S. House of Representatives n.d., p.4).

In a recent Congressional Testimony, TSA Administrator, John Pistole stated, “The vast majority of 628 million annual air travelers present little to no risk of committing an act of terrorism, we should focus on those who present the greatest risk, thereby improving security and the travel experience for everyone else.” (Transportation Security Administration, 2011) It was found that passenger revenue (nearly 80%) comes from domestic travel. It was also found that a relatively small group of travelers (frequent flyers who take more than 10 trips a year) account for a significant amount of travel. While this small group of flyers represent only 8% of the total number of passengers flying in a given year, they make up almost 40% of trips taken (www.avjobs.com/history/airline-economics.asp, 2012). This explains how the majority of the traveling public are trustworthy travelers who pose little or no threat to the current aviation enterprise in the United States. Using a technology enhanced risk-based passenger-screening program that validates the identification of known trustworthy passengers and processes them in a more expeditious manner will improve the current RBS aviation security passenger-screening program. Additionally, trustworthy passengers under the RBS aviation passenger-screening program will be subject to less scrutiny of inspection than high risk and unknown traveling

passengers. Incorporating biometric technology that validates an individual's identification will improve the efficiency and effectiveness of the screening system. At the same time, the RBS model will reduce required federal resources, lessen the frustration of current passenger travel experience and be financially advantageous to both the airline industry and the U.S. economy. There are many benefits to incorporating and leveraging current biometric technologies into the TSA's current Risk-Based Screening aviation passenger screening program.

Since September 11, 2001, the commercial passenger screening process has been drastically transformed into a rigid methodical one-size-fits-all passenger-screening security program. The system applies an "equal risk" model to all passengers and does not differentiate between suspected terrorists or the 1M-mile frequent flier. The TSA struggles to strike a balance between effectively screening passengers and avoiding undue delays and hassles to the traveling public while trying to prepare for the next attack on the system. The current strategy for the passenger-screening approach at federalized airports is a "one-size-fits-all" screening approach for all passengers, which is woefully ineffective. The Transportation Security Administration "inspects everyone and everything" the same way no matter their status, stature, race, age or creed. The strategy for passenger screening is each traveler is treated equally as a threat so all are scrutinized and screened the same way. Each individual goes through the same regimen of a "one-size-fits-all" passenger-screening program. This program has been an extremely successful strategy, but is not beneficial to the traveling public, governmental budgets or U.S. economy because of its inefficiencies.

Every day in the United States, approximately 2 million air travelers travel throughout the country and are subjected to a one-size-fits-all screening system. This passenger screening process uses massive amounts of resources, creates frustration amongst the traveling public, and is not an effective or efficient way to conduct passenger screening. The aviation passenger-screening program has been successful, but it is costly and inefficient for the traveling public. The TSA annually spends about $7 billion and has a workforce numbering an estimated

60,000. One reason for the workforce and expense being so large is that screening functions are imposed virtually uniformly on every traveler and airport in the United States (Riley, 2004, p.24). The TSA is continually adding to the number of new passenger screening security procedures at each checkpoint, which contributes to large annual increases in the TSA's budget. For example, from fiscal year 2004 through fiscal year 2010, the TSA's annual budget increased by almost 70% from $4.5 billion to $7.6 billion while airline loads are stable (U.S. Travel Association, n.d. p.8).

In recent surveys it was found the American traveling public travels less because of the frustration they feel when having to deal with the current aviation passenger-screening processes. A majority of the individuals surveyed stated they would take more flights every year if the screening process remained as effective as it was but was less intrusive and less time-consuming. In 2008, a survey found the hassles of air travel were discouraging people from flying. More than 28% of the respondents said that they choose to avoid one trip a year. A simple extrapolation of these results indicated that 41 million travelers, or slightly more than 100,000 per day avoid trips during the year. That loss of travel translates into a $26.5 billion loss to the U.S. economy; including $9.4 billion to airlines, $5.6 billion to hotels, $3.1 billion to restaurants, and $4.2 billion in federal, state and local tax revenues. A similar 2010 survey found that 64% of travelers surveyed stated, that on average they would take two to three more trips a year if the hassle could be reduced without compromising security effectiveness. These additional trips could add an estimated $84.6 billion in spending and possibly almost 900,000 jobs to our economy (U.S. Travel Association, n.d., pp. 6–7).

TSA administrator, John Pistole, believed the former passenger screening security model was inefficient (Yager, 2011). There is a better way to conduct passenger screening that is more effective and efficient, as well as being customer friendly while meeting the needs of the traveling public. In the fall of 2011, the introduction of the TSA's new Risked Based Security (RBS) has rapidly

introduced new passenger-screening programs to compliment the current aviation passenger-screening program.

B. CASE FOR UTILIZING BIOMETRICS IN PASSENGER SCREENING

1. Resources

Incorporating biometric technology into the current RBS aviation passenger screening program could lessen the amount of resources required for aviation screening or reprioritize current aviation screening resources to higher risk or threat passengers. Today, the TSA is introducing a risk-based screening initiative, but still utilizes a "one-size-fits-all" approach for the majority of passenger screening. Additionally, the TSA is continually adding to the number of new passenger screening security procedures at each checkpoint, which contributes to large annual increases in the TSA's budget. For example, from fiscal year 2004 through fiscal year 2010, the TSA's annual budget increased by almost 70% from $4.5 billion to $7.6 billion. (U.S. Travel Association n.d. p.8)

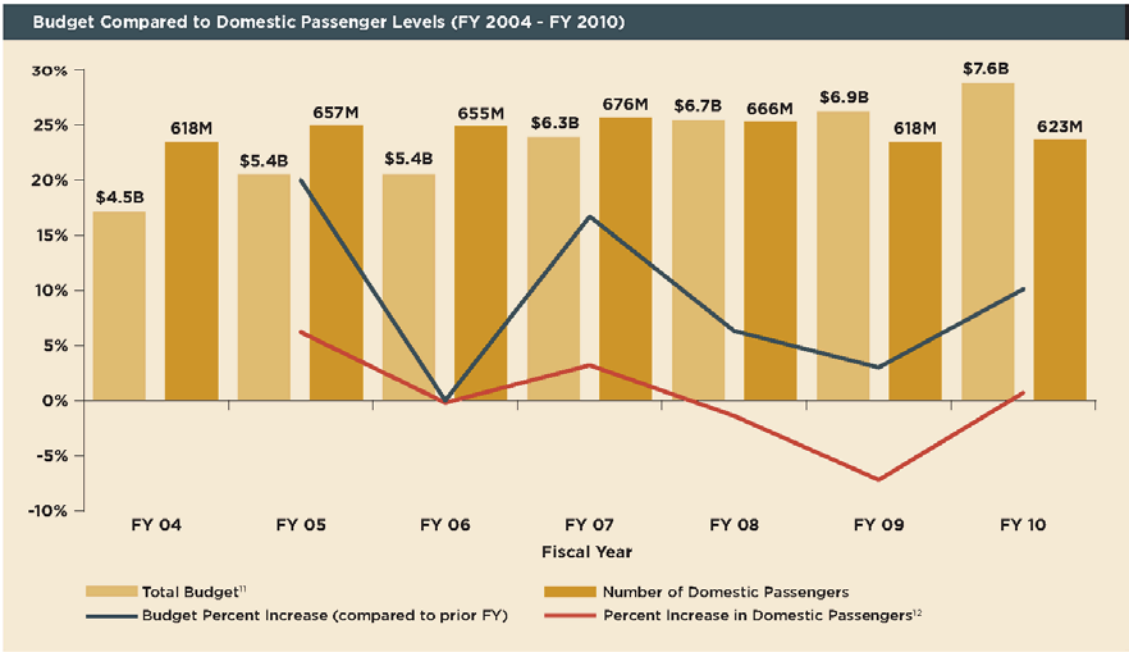

Figure 1. TSA Budget compared to domestic passenger levels from U.S. Travel, n.d.

By lessening this aviation passenger-screening burden created by the one-size-fits-all, each passenger is treated the same, so low risk passengers receive the same screening rigor as high and unknown risk passengers. The current resources, both personnel and equipment, are uniformly distributed across aviation screening checkpoints but could be refocused and re-prioritized toward the unknown and high risk or threat passengers. Many efficiencies can be gained by incorporating biometric technology and the RBS screening system for all airports; less equipment would be required; fewer Transportation Security Officers (TSO) would be required, which would lead to a budgetary savings by gaining efficiencies and effectiveness through technology and risk management.

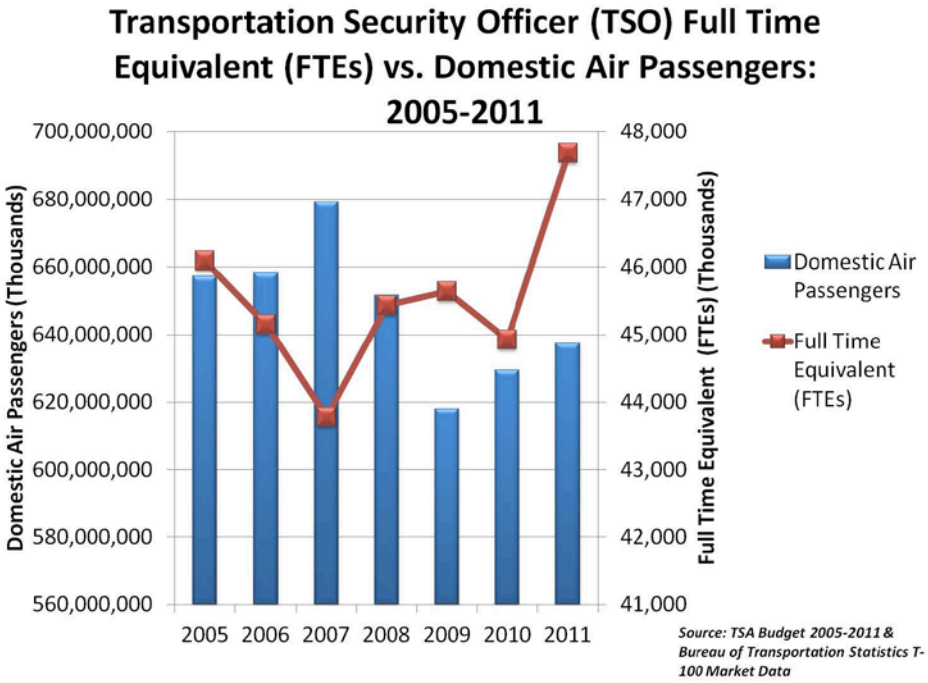

Figure 2. FTE vs. Domestic Air travel from U.S. House of Representatives, 2012

2. Statutory Requirement

Another reason for incorporating biometric technology into the current aviation passenger-screening program is both Congress and the President enacted statutory and directive requirements to incorporate biometric technology

into the airport screening processes. Congress included statutory language in the 2001 Aviation and Transportation Security Act (ATSA; P.L.107–71) and also in the fiscal year 2008 Consolidated Appropriations Act (P.L. 110–161) directing the TSA to establish a domestic and international “trusted traveler” program that incorporates biometrics technologies (Elias, 2009, pp. 20–22). In June 2008, the White House published NSPD-59 and HSPD-24, which requires biometrics for identification and screening to enhance national security. The directive provides a federal framework for applying existing and emerging biometric technologies to the collection, storage, use, analysis, and sharing of data identification to improve screening process and procedures employed by agencies and to enhance national security (The White House 2008, p.1). Additionally, in a recent congressional majority staff report, Congress recommended the TSA must develop an expedited screening program using biometric credentials that would allow the TSA to positively identify trusted passengers and crew members so that the agency could prioritize its screening resources on unknown and high risk passengers and select individuals. The TSA will not be able to function as a truly risk-based organization until the agency can differentiate between passengers based on risks (U.S. House of Representatives n.d. pp.13 and 20).

3. Economics

A final purpose for incorporating biometric technology into the aviation passenger-screening program is that it could add economic growth to the travel and airline industry while potentially producing more jobs in United States. In recent surveys it was found the American traveling public travels less because of the frustration they feel when having to deal with the current aviation passenger screening process. A majority of the individuals surveyed stated they would take more flights every year if the screening process remained as effective as it was but was less intrusive and less time-consuming. In 2008, a survey found the hassles of air travel were discouraging people from flying. More than 28% of the respondents said they choose to avoid one trip a year. A simple extrapolation of these results indicated that 41 million travelers, or slightly more than 100,000 per

day avoid trips during the year. These additional trips could add $84.6 billion in spending and possibly almost 900,000 jobs to our economy (U.S. Travel Association n.d. pp. 6–7). The FAA predicts that yearly passenger totals will grow from approximately 713 million domestic and international passengers in FY 2010 to 731 million in FY 2011. In the next five years alone, FAA predicts that passenger levels will grow by an average of 3.7 percent per year, and continue to grow at an average of 2.5 percent from FY 2016 to FY 2032. Passengers are projected to increase an average of 2.5 percent a year, with regional carriers growing at a slightly higher rate than their mainline counterparts. By 2032, U.S. commercial air carriers are projected to fly 1.9 trillion ASMs (Available Seat Miles) and transport 1.23 billion enplaned passengers a total of 1.57 trillion passenger miles (FAA, 2012, p.38). With such steep rises in passenger levels, TSA will be hard pressed to control the growth of its budget; wait times at security checkpoints will increase, and the burdens of the current system will slow economic recovery unless Congress and TSA develop a long-term, risk based strategy to focus assets and resources at the highest priority threats (U.S. Travel Association n.d. p.8).

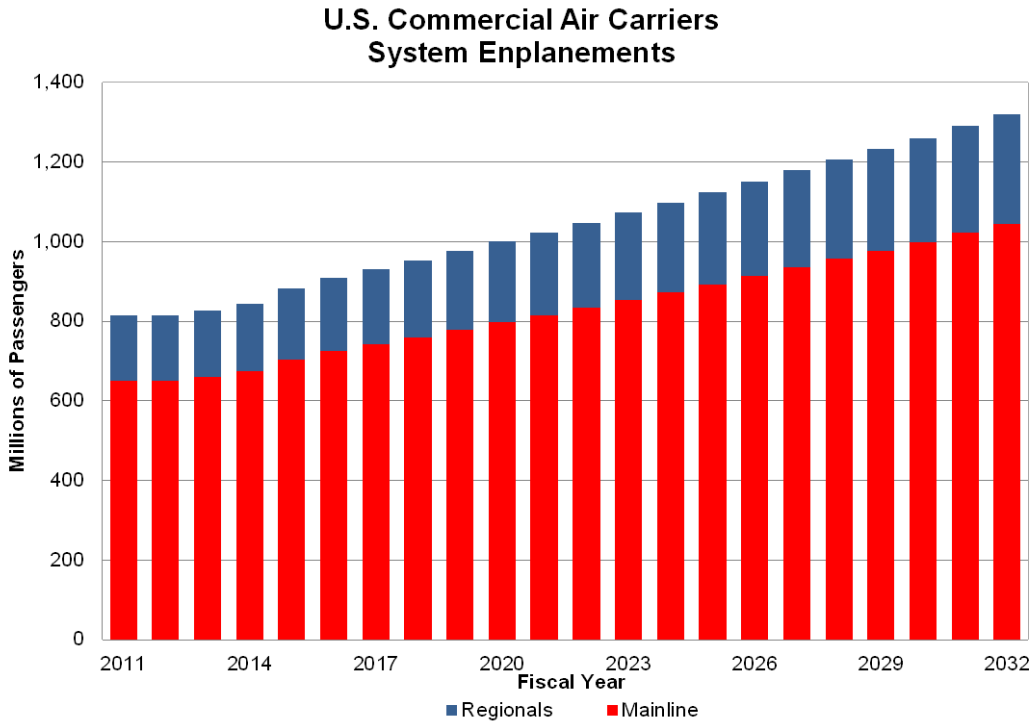

Figure 3. FAA's Forecast of Enplanements from 2011–2032 from FAA, 2012

C. DEFINING THE PROBLEM

The current aviation passenger-screening program utilizes a 72-hour pre-screening process, called Secure Flight along with observation and interaction of traveling passengers called Screening of Passengers by Observation Techniques (SPOT) conducted by Behavior Detection Officers (BDO) to determine the level of scrutiny they will go through the screening process when arriving at the airport. These traveling passengers may be put into a low risk, unknown risk, or high-risk category based on the afore mentioned formula. Those in the low risk category will receive fewer screening procedures and are considered "trusted travelers" whereas the other passengers will be considered for more scrutiny in the screening process. The new RBS initiative utilizes intelligence-driven screening processes and individual observation to determine the proper level of screening that matches the passenger's risk assessment.

Remarkably, the current aviation passenger-screening program does not utilize or integrate biometric technology to validate a person's identity during the screening process. During the aviation passenger-screening process, a passenger's identification documentation itself is authenticated, but this does not guarantee the true identity of the passenger. A passenger's identification documentation is authenticated but their identity is not validated. The increased sophistication of document forgery is making it more difficult to guarantee the genuineness of a passenger's travel documentation. The true identity of a passenger has always remained in question. A much more reliable and efficient way to validate a person's identity is through biometrics. Incorporating biometrics could greatly enhance effectiveness and provide greater reasonable assurance of the passenger's true identity especially in low risk traveling public populations.

It is important to investigate how to improve the Risk-Based Security initiatives for APSP procedures for the United States. Other agencies, both private and governmental, are incorporating biometric technologies to improve, enhance, and leverage technology to improve the efficiency, reliability, and effectiveness of security models. Further investigation merits graduate-level research to examine how biometric technologies can be utilized to improve the current RBS aviation passenger-screening procedures. There may be a "better way of screening " model that can validate an individual's identity and not just prove the authenticity of their identification documentation. This research can contribute to a better aviation passenger-screening program by complementing the current RBS initiatives while demonstrating better screening procedures utilizing biometrics to gain synergy for the Risk-Based Security aviation passenger-screening procedures.

Incorporating biometrics into the Risk-Based Security aviation passenger-screening program could improve the current passenger screening system by making it more effective and efficient, customer friendly as well as economically feasible for commercial aviation in meeting both the needs of the traveling public and requirements of the regulatory statutes. The new TSA Risk-Based Security

aviation passenger-screening program for the United States federalized airports plays an important role in the transportation security sector of the aviation security domain.

The decade-old aviation security passenger-screening method of the “one-size-fits-all” passenger-screening program is changing to a novel Risk-Based Screening program in an attempt to improve efficiency and effectiveness of passenger screening. There is a better way to leverage biometric technology to improve the RBS aviation passenger-screening program’s efficiency and effectiveness in regard to the identity of the travelling public. Its public acceptability and customer friendliness that is economically sensible, decreases resources required while improving risk mitigation and meeting statutory compliance.

D. RESEARCH QUESTION

1. Primary Research Question:

How could biometric technologies enhance the current Risk-Based Security (RBS) aviation passenger-screening program for the federalized airports in the United States to improve passenger identity authentication?

2. Secondary Research Questions:

How are current aviation passenger-screening program procedures being adapted to enable risk-based security initiatives?

What biometric technologies currently used by other governmental agencies can be incorporated to improve passenger identity authentication?

How could TSA integrate biometric technologies into the risk based screening programs and the current aviation passenger-screening program?

E. SUMMARY

It is important to investigate how to improve the Risk-Based Security aviation passenger-screening program for the United States. Other agencies,

both private and governmental, are incorporating biometric technologies to improve, enhance, and leverage technology to improve the efficiency, reliability, and effectiveness of security models. I believe further investigation merits graduate-level research to show how biometric technologies can be utilized to improve the current RBS aviation passenger-screening program.

The TSA will continue to address the tension between sensibly screening passengers and crewmembers while avoiding undue delays to the traveling public, minimizing economic impact on the airline industry and the U.S. economy, being compliant with statutory legislation and directives while being publicly and socially acceptable. The current aviation security passenger-screening program has been a program of “one size fits all” since the tragic events of 9/11. This program has been woefully inefficient and has impacted the way United States citizens travel, which has caused an impact on the economy of the United States.

During the aviation passenger-screening process, a passenger’s identification documentation is authenticated but their identity is not validated. Incorporating biometrics will greatly improve efficiency and effectiveness while providing a greater reasonable assurance of the passenger’s identity especially in the low risk traveling public population. The TSA must develop an expedited aviation passenger-screening program using advanced biometric technology that allows the TSA to positively identify low risk “trusted” passengers and crewmembers so the agency can prioritize it’s screening resources on individuals of high risk while speeding up the screening process (Peterman, Elias and Frittelli 2011 p.65). Biometrics technology will lead to a better way.

II. LITERATURE REVIEW

A. INTRODUCTION

The purpose of this review is to examine the current RBS passenger-screening program, review current biometric technology and highlight current incorporation of biometrics into RBS initiative programs. The scope of the literature review examines three broad categories 1.) Risk Based Security Initiative 2.) Current Biometric Technology 3.) Governmental and Non-Governmental biometrically enhanced security programs. The sources of the literature review include government and non-government information from: online articles, policy documents, scholarly journal articles, Congressional research papers, white papers, Congressional testimony, and academic research including interview with leading policy makers in the biometrics. The literature examined has been within the past ten years and the most recent articles dated May 2012. The purpose of this literature review is to review issues and programs that could enhance the current RBS passenger-screening model and are relevant to making our aviation passenger security screening system more effective and efficient.

B. RISK BASED SECURITY

Since September 11, 2001, changes have been made to aviation security in an effort to prevent future terrorist attacks. Additional screening processes have been put in place and new technologies have been deployed. This is reflected in the budgets for the aviation elements of the TSA. As these changes have occurred, however, questions have been raised about a basic philosophy of aviation security applied uniformly to all. This argument has been “crystallized” in the public debate with images of grandmothers getting the same treatment as people who are more likely to be terrorists. One outcome of this debate has been renewed interest in ways to vary the amount of screening individuals receive with the goals of improving performance and reducing the security burden on (some)

travelers. Preferential treatment in screening can be approached in two ways. The first is identifying individuals who may pose *more* risk than others and allocating more security resources to them, a process usually called *profiling*. The second is identifying individuals who likely pose *less* risk than others and allowing them to pass through security with reduced security screening, a process known as *trusted traveler programs* (Jackson, Chan, LaTourrette, 2011, pp. 1–2).

There is extensive literature examining the profiling, but there is much less analysis of the trusted traveler programs. Creating a new Trusted Traveler (TT) program that utilizes true risk-management requires a controlled enrollment and re-verification process; a confirmation process at the airport that ensures only enrolled individuals are utilizing the TT screening lanes and a checkpoint process that reflects the low-risk nature of the traveler (U.S. Travel Association, n.d. p. 12). The basic logic of a trusted traveler program is that security resources can be shifted from travelers who have been confirmed as low risk to the remaining unknown-risk population. It is assumed that devoting more security resources to the unknown-risk population would increase the chance of identifying individuals seeking to bring weapons through security checkpoints to stage attacks on aircraft (Jackson, Chan, LaTourrette, 2011, pp. 1–2). The trusted traveler programs apply the same logic applied to TSA employees. At many airports, TSA employees are screened neither the first time nor subsequent times when they enter the secure sterile area of an airport throughout the course of the day because they have had a background check and are trusted. The TSA employees are thought to be practically low risk for coercion or vulnerable to radical influence to which passengers are thought to be vulnerable. Additionally, at many other airports, background checked employees (airport shops, airport police, airport kiosk volunteers) are considered low risk and have unibiometric all-access badges that allow them to bypass screening security and enter into the sterile secure area (Riley, 2011, pp. 4–5). This has been the precedent for many years and there have been no terrorist incidents associated with this model

indicating a passenger trusted traveler program could be successful utilizing a similar methodology.

In a recent RAND Corporation report *"Assessing the Security Benefits of a Trusted Traveler Program…"* found that the key elements needed for a trusted traveler program are:

- A member of the traveling public applies for the program, so the program is voluntary and may involve an application fee.
- A tightly controlled background-check process verifies that the individual meets the criteria for trusted status.
- A separate, reduced security-screening process is applied to trusted travelers when they access air transportation, thus reducing resources needed for screening (Jackson, Chan, LaTourrette, 2011, pp.1–2).

The reduction in screening undergone by a trusted traveler would free up resources that could be applied to members of the general public. If screening resources are treated as a constant, all resources could be removed or fewer resources could be used from the "trusted traveler lines" and would be redeployed to "general public lines," affording, for example, more time to scrutinize x-ray images of their belongings or manually search their bags, more resources to deploy and routinely use explosive detection technologies that are more effective than current methods. In order to have a trusted traveler program with all resources being constant, risk-based security must be weighed heavily for the aviation passenger-screening program (Jackson, Chan, LaTourrette, 2011, pp.1–2).

In the fall of 2010 Transportation Security Administration (TSA) Administrator John Pistole directed the agency to explore ways to develop a strategy for a "Trusted Traveler" program. The new strategy formulation needed to examine the procedures and technologies TSA used, how specific security procedures were carried out, and how screening was conducted. The exploration

resulted in the novel Risked Based Security initiatives. While TSA is currently implementing new risk-based security initiatives, TSA must continue to assess its programs to evolve the passenger screening security model to stay ahead of tomorrow's security threats (Transportation Security Administration, n.d.).

In 2011, TSA Administrator Pistole introduced Risk-Based Security (RBS) initiatives to the TSA and the general public. To this end, the TSA is examining new security protocols to improve the passenger screening models at selected airports throughout the United States by applying a new risk-based security pilot program. Some of the guiding principles of Risk Based Screening initiatives are:

- The majority of airline passengers are low risk.
- By having passengers voluntarily provide more information about them, TSA can better segment the population in terms of risk.
- TSA must accelerate its efforts to optimize screening processes and use of technology to gain system-wide efficiencies.
- TSA must better calibrate operational responses and procedures to specific threat information.
- The RBS pilot program efforts will enhance security of the nation's aviation system (Transportation Security Administration, 2011).

In general, RBS initiatives use information gained during pre-screening, along with a thorough observation and interaction with passengers to determine the proper level of screening that matches the passenger's risk assessment. Risk-Based Security allows the TSA to re-focus resources on higher risk or unknown risk travelers thereby increasing security (Transportation Security Administration, n.d.). In Risk-Based Security, the TSA takes into account the possible threat, vulnerability, and potential consequences of all associated airline and travel industry passengers and employees. The TSA applies these risk-based methodologies in order to depart from the "inspect everyone and everything" and the "one-size-fits-all" approaches to screening (Riley, 2011, p. 153). Using these risk-based methodologies, the TSA improves checkpoint

efficiency while decreasing passenger wait times and providing cost savings to the U.S. taxpayer. In a similar program, CBP's Global Entry Program, allows low-risk pre-approved travelers expedited access into the U.S. utilizing biometric Global Entry kiosks at airports rather than having travelers wait in line for border and customs clearance. As of mid-2012, there were Global Entry kiosks at 25 major airports that had been used over 2.6 million times reducing the traveler wait times by 70% and saving CBP officers over 50,000 inspection hours allowing them to focus resources on individuals of unknown or high risk status (Zuckerman, 2012). The TSA RBS initiative is based on the premise that the majority of airline passengers are low-risk and TSA knows who they are. The more information available on each traveler, the better his/her risk category can be determined. Incorporating risk-based initiatives with technology can optimize the screening process and efficiency can be gained through risk mitigation while increasing security by focusing on the unknowns (Transportation Security Administration, 2012). In fast-tracking passenger screening processes, the RBS initiatives that are expediting passenger screening benefits for qualified "trusted travelers" include no longer removing: 1.) Shoes 2.) 3–1–1 compliant[1] bags from carry on 3.) Laptops from bags 4.) Light jackets and over garments and 5.) Belts (Transportation Security Administration, 2012).

[1] 3-1-1 compliant is 3.4 ounce (100ml) bottle or less (by volume); 1 quart-sized, clear, plastic, zip-top bag; 1 bag per passenger placed in screening bin. One-quart bag per person limits the total liquid volume each traveler can bring. 3.4 ounce (100ml) container size is a security measure.

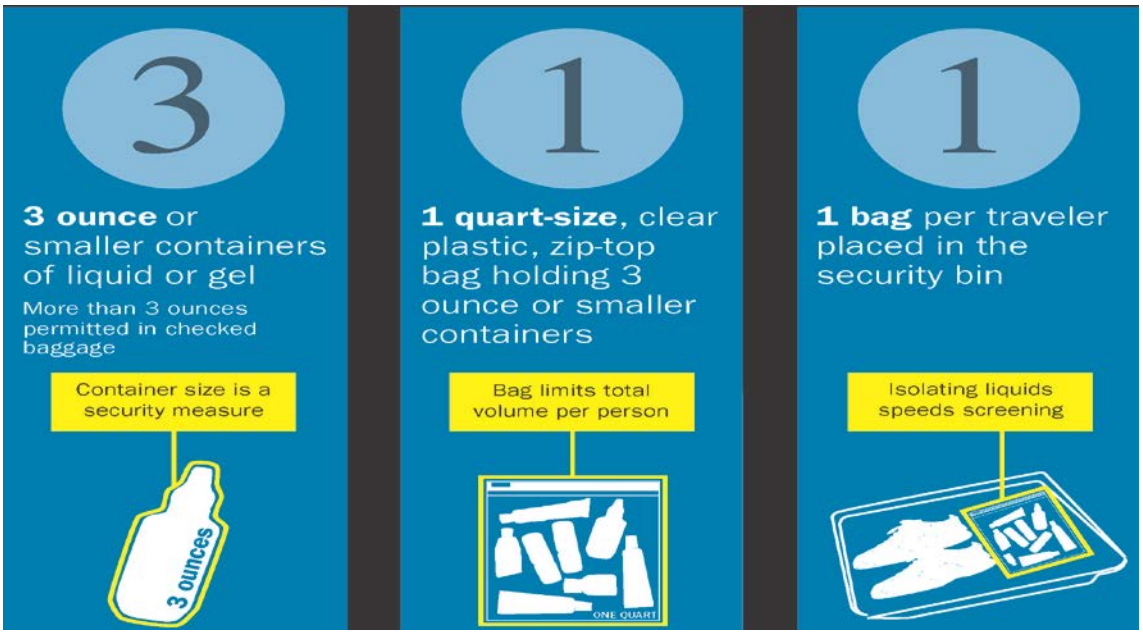

Figure 4. TSA 3–1–1 Policy from TSA, 2012

C. TSA RISK BASED INITIATIVES

The TSA Administrator, John S. Pistole has taken major steps required to incorporate risk-based security initiative passenger screening. In his testimony in June 2011, he testified to Congress:

> We [TSA] are working to expand our ability to conduct more risk and identity-based screening. This is evident in our work on a new crewmember screening system. We are currently testing an identity-based system to enable TSA security officers to positively verify the identity and employment status of airline pilots. We hope pilots are responsible for the safety of the traveling public every time they fly a plane. It just makes sense to treat them as trusted partners, as well (Department of Homeland Security, 2011).
>
> John S. Pistole, Administrator TSA

Figure 5. Risk Based Security Initiatives from TSA, 2012

The Risk-Based Security Initiatives passenger-screening model has introduced new expediting screening programs, which are: 1. Pre-Check (TSA Pre✓™) - Expedited Screening 2.) Screening for Passengers 12 and Under 3.) Screening for Passengers 75 and Older 4.) Screening for Department of Defense Common Access Card (DoD CAC) U.S. Service Members 5.) Known Crew Member (KCM). (Transportation Security Administration, 2012)

1. Pre-Check (TSA Pre✓™) Expedited Screening:

TSA Pre✓™ involves screening select frequent fliers as well as, members of Customs and Border Protection and various trusted traveler programs. The Pre✓™ travelers voluntarily sign up for this program, go through a thorough background check and provide photo identification. This makes the trusted travelers eligible to go to a separate screening lane and receive expedited

passenger screening benefits.[2] TSA Pre✓™ enhances aviation security by placing more focus on pre-screening individuals who volunteer to participate in order to expedite the travel experience and passenger screening process (Transportation Security Administration, 2012).

2. Screening for Passengers 12 and Under:

Passengers 12 and under are allowed to leave their shoes on during screening. They are permitted multiple passes through the walk-through metal detector (WTMD) and advanced imaging technology (AIT/ATR). They are subjected to a greater use of explosives trace detection (ETD) technology to clear any alarms in lieu of being subjected to a pat down. These new procedures ensure effective security and allow TSA to focus its resources on individuals the agency knows less about while improving travel experiences for younger travelers (Transportation Security Administration, 2012).

3. Screening for Passengers 75 and Older:

Passengers 75 and older are also allowed to leave their shoes on during screening, as well as, multiple passes through the WTMD or AIT/ATR and utilized the ETD to clear any alarms. The new processes for passengers 75 and older ultimately reduce – but not eliminate – pat-downs that would have otherwise been conducted to resolve anomalies. If anomalies are detected during security screening that cannot be resolved through other procedures, it is possible they may be subject to a modified pat down. Again, this is another example of utilizing finite resources on passengers who may be more likely to pose a risk to transportation while expediting the passenger screening process.

4. Department of Defense Common Access Card (DoD CAC):

The members of the U.S. Armed Forces are entrusted to protect the security and values of citizens with their lives and as such, these members pose

[2] TSA Pre✓™ participants use dedicated screening lanes for screening benefits which include leaving on shoes, light outerwear and belts, as well as leaving laptops and 3-1-1 compliant liquids in carry-on bags.

very little risk to aviation security and are considered “trusted travelers.” Eligible service members include U.S. Armed Forces service members including Reservist and National Guard members, who possess a valid Department of Defense Common Access Card (DoD CAC). Service members in good standing with the Department of Defense (DoD) will receive expedited screening benefits and will be directed to the TSA Pre✓™ expedited screening lane after their status has been verified. Again, this will also expedite the passenger screening process (Transportation Security Administration, 2012).

5. Known Crewmember (KCM):

KCM incorporates airline pilots as “trusted partners” in the aviation security strategy. This program allows identity confirmed airline pilots to bypass passenger-screening procedures and proceed to the gate and their aircraft duties. Currently the crewmembers enter a screening checkpoint and provide their airline ID, which is matched against a database called Cockpit Access Security System (CASS). If the pilot’s picture ID matches the CASS picture, the pilot is granted access to the secured gate areas without being screened. This is very similar to TSA employees not being screened when they enter the secure gate area of an airport throughout the course of the day, because they are “trusted employees” who have passed a thorough government background check, provided a biometric fingerprint with high resolution digital photo, and are thought to have a particularly low risk threat to aviation security. In addition to the TSA employees, numerous other airport employees, who have undergone the same scrutiny as the TSA employees, such as airport police department personnel, enter the secure area of the airport without going through screening procedures (Riley, 2011, pp. 153–154). This methodology is being applied to the KCM program to relieve the volume burden upon security checkpoints and improve the efficiency of our passenger screening approach.

6. Expanded Behavior Detection:

Expanded Behavior Detection builds on the existing Screening of Passengers by Observation Techniques (SPOT) program, which has grown since 2003 to include over 160 airports. Under the Expanded Behavior Detection pilot program, TSOs employ specialized behavioral analysis techniques to determine if a traveler should be referred for additional screening at the checkpoint. The vast majority of passengers at the pilot airport checkpoints experience a “casual greeting” conversation with a Behavior Detection Officer (BDO) as they pass through travel document verification. This additional interaction, used by security agencies worldwide, enables officers to better verify or dispel concerns about suspicious behavior and anomalies (U.S. Department of Homeland Security, 2012).

7. Passenger Screening Canines:

This is part of RBS that provides support for the development, training, certification and deployment of canine programs. Each canine team consists of a specially trained dog and a Federal, State, or local handler. This program, in partnership with State and local law enforcement agencies, provides a mobile response platform for threats to transportation security, including threats within the mass-transit commuter-rail, and maritime-ferry transportation sectors. This has now been expanded to airports where these canine teams will have presence and assist with the passenger-screening process (www.tsa.gov).

8. Honor Flights:

TSA implemented new procedures for passengers on Honor Flight Network flights. The new procedures greatly reduce screening procedures conducted on participating WWII veterans and their escorts. These screening procedures reduce but do not eliminate, screening requirements on Honor Flight Network flights (www.tsa.gov).

9. Secure Flight:

Secure Flight is a behind-the-scenes program that enhances the security of domestic and international commercial air travel through the use of improved watch list matching. By collecting additional passenger data, it improves the travel experience for all airline passengers, including those who have been misidentified in the past. When passengers travel, they are required to provide the following Secure Flight Passenger Data (SFPD) to the airline: name, date of birth, gender and redress number (if applicable). The airline then submits this information to Secure Flight, which uses it to perform watch list matching. This serves to prevent individuals on the NO Fly List from boarding an aircraft and to identify individuals on the Selectee List for enhanced screening. After matching passenger information against government watch lists, Secure Flight transmits the matching results back to airlines so they can issue passenger boarding passes (www.tsa.gov/stakeholders/secure-flight-program).

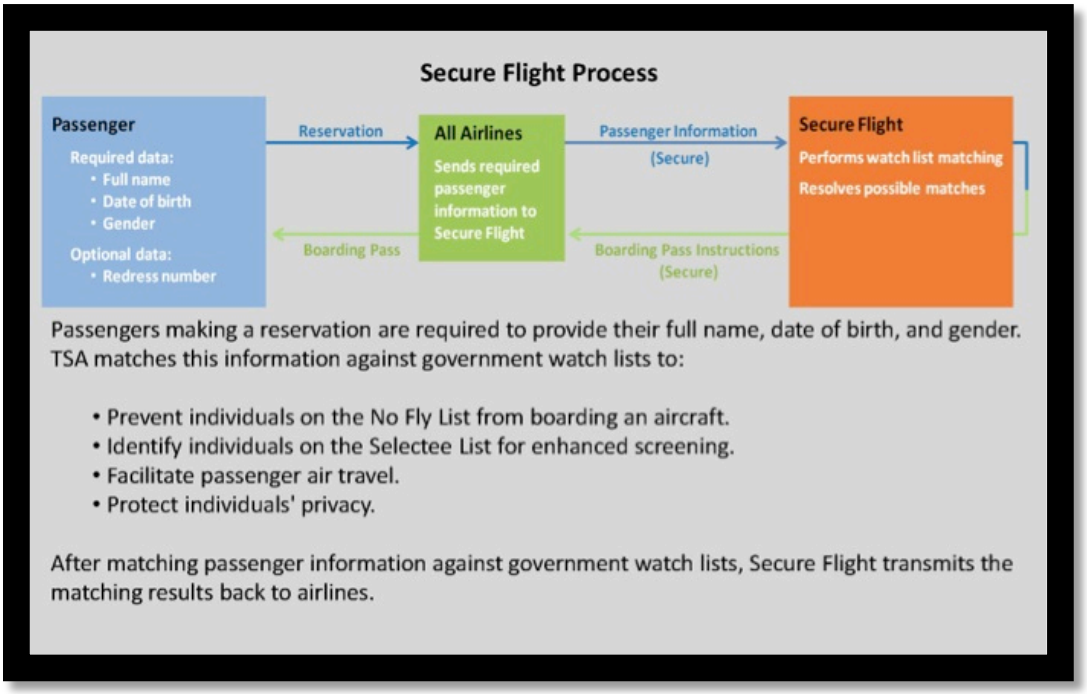

Figure 6. Secure Flight Program Overview from TSA, 2012

D. BIOMETRIC TECHNOLOGY

From the Merriam-Webster dictionary: "*biometrics is the measurement and analysis of unique physical or behavioral characteristics (as fingerprint or voice patterns) especially as a means of verifying personal identity*." The National Science and Technology Council (NSTC) Sub Committee on Biometrics provides the origins of biometrics; the term "biometrics" is derived from the Greek words "bio" (life) and "metrics" (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago (National Science and Technology Council, 2008, p.55).

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into once small communities. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis (National Science and Technology Council, 2008, p.56).

Biometrics is a tool for the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways.

Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, service, and to other rights or

benefits, including the ability to cross international borders. The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud and enhancing public safety and national security (National Research Council of the National Academies, 2010, p1).

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, biometrics is a measurable biological and behavioral characteristic that can be used for automated recognition. A few of the current biological characteristics, commonly referred to as modalities, used to identify people are fingerprints, iris images, facial photos certain types of voice patterns, palm prints, and DNA. Behavioral characteristics / modalities can be a signature, the keystroke pattern on a keyboard, certain types of voice patterns, and gait (Center for Army Lessons Learned (CALL, 2011, p.45). The most common biometric modalities are: face, fingerprints, hand geometry, iris, voice, signature, gait, and keystroke (National Research Council of the National Academies, 2010 pp.31–34).

Looking at biometrics as a process is an automated method of recognizing an individual. Biometrics as a process is used in two ways: verification and identification. Verification compares one biometric to an identified biometric (1:1) to verify that an individual is who he says he is. Identification compares one biometric to a database of biometrics (1:N) to find out who an individual is (Center for Army Lessons Learned (CALL), 2011, p45). When looking at the use of biometrics as a process, it is a series of procedures within a system. The functioning of a basic biometric system is a multi-step method where, in general, an individual presents a characteristic of himself or herself; then that characteristic(s) is captured by a sensor and converted into an algorithm sample; that sample is then compared to reference sample or baseline algorithms in a database; the conclusion of the process is the a match and non-match which allows a corresponding action such as entry into a secure structure. Systems that

perform biometric recognition exist within a constellation of other authentication and identification technologies and offer some distinct capabilities.

Authentication technologies are typically based on one of three things: Something the individual knows, such as a password; 2. Something the individual has, such as a physical key or secure token; 3. Something the individual is or does. Biometric technologies employ the last of these. Unlike password or token-based systems, biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place. One important difference between biometric and other authentication technologies, such as tokens, or passwords, is that these other technologies place trusts in cooperative users, allowing them to produce what they possess or demonstrate what they know (through dependence on the user's safekeeping of a token or password). These other forms of authentication do not protect against the sharing or transfer to the token or secret, whereas biometric traits are tied to an individual—specifically something an individual is or does (National Research Council of the National Academies, 2010, pp.5–6).

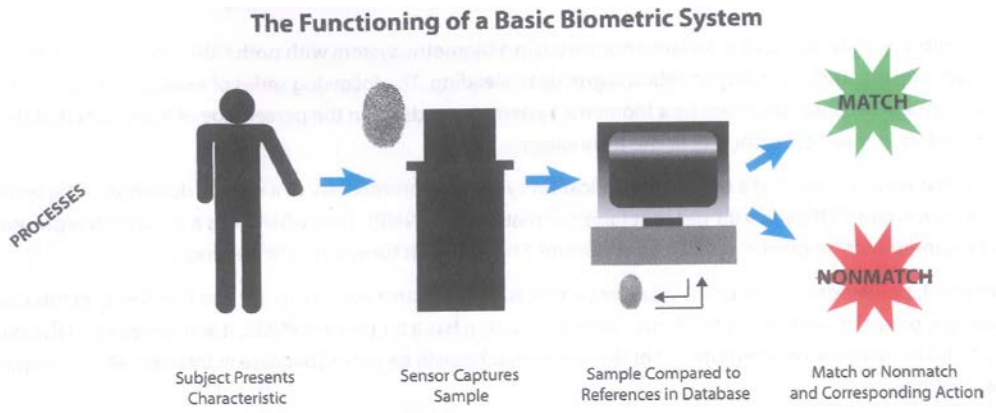

Figure 7. A Basic Biometric System from National Academy of Sciences, 2010

Biometrics as a systems that are presently in use, typically use a single biometric trait or single modality (unibiometric) to establish identity. A recent trend in biometrics involves a shift from unibiometric to multibiometric systems. Unibiometric systems make use of a single source of biometric information to

perform identity determinations (verification, identification, negative recognition, etc.). Both theoretical research and empirical observation of fielded systems reveal that single modal unibiometric systems are subject to a variety of shortfalls. Ceilings on performance accuracy, poor subject population coverage, relatively high failure-to-enroll rates, and ease of circumvention are classic examples of such shortfalls. Some of the limitations of a unibiometric system can be addressed by designing a system that consolidates multiple sources of biometric information. This can be accomplished by fusing, for example, multiple traits of an individual or multiple feature extraction and matching algorithms operating on the same biometric. Multi-biometric systems, which rely on more than one source of biometric input, can be used to alleviate such shortfalls. Arguably, such systems may also include other sources of information including biographic, travel document-based, etc. (Ross, 2007, P1)

Combining multiple sources of biometric information and databases has created a biometric fusion, which is the use of multibiometric inputs or methods of processing to improve performance. The traditional role of multibiometric fusion has been to increase system accuracy, increase the coverage across the population base, decrease instances of failures to acquire / failures to enroll, and increase the difficulty associated with circumvention. These four purposes directly relate to a subset of the characteristics typically used to evaluate a biometric modality. In evaluating multibiometric modality systems, Jain and Ross, leaders in the biometric field, initially came up with the characteristics to evaluate biometric systems. The characteristics that are commonly utilized to evaluate a biometric system are: universality, uniqueness, permanence, measurability, performance, acceptability, and circumvention (Bartlow, Nick and Zekster, Gregory,2009 p.2).

The National Science and Technology Council (NSTC) Sub Committee on Biometrics provides the origins of biometrics; the term “biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure). Automated biometric systems have only become available over the last few decades, due to significant

advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago (National Science and Technology Council, 2008, p.55).

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into once small communities. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis (National Science and Technology Council, 2008, p.56).

Today, Biometrics is seen as the automated recognition of individuals based on their behavioral and biological characteristics. It is a tool for establishing confidence that one is dealing with individuals who are already known (or not known)—and consequently that they belong to a group with certain rights (or to a group denied certain privileges). It relies on the presumption that individuals are physically and behaviorally distinctive in a number of ways. Biometric systems are used increasingly to recognize individuals and regulate access to physical spaces, information, service, and to other rights or benefits, including the ability to cross international borders. The motivations for using biometrics are diverse and often overlap. They include improving the convenience and efficiency of routine access transactions, reducing fraud and enhancing public safety and national security (National Research Council of the National Academies, 2010, p. 1).

1. Biometrics as a Characteristic or Process

Biometrics is a general term used alternatively to describe a characteristic or a process. As a characteristic, biometrics is a measurable biological and behavioral characteristic that can be used for automated recognition. A few of the current biological characteristics, commonly referred to as modalities, used to identify people are fingerprints, iris images, facial photos certain types of voice patterns, palm prints, and DNA. Behavioral characteristics / modalities can be a signature, the keystroke pattern on a keyboard, certain types of voice patterns, and gait (Center for Army Lessons Learned, 2011, p. 45). The most common biometric modalities are:

Face—Static or video images of a face can be used to facilitate recognition. Modern approaches are only indirectly based on the location, shape, and spatial relationships of facial landmarks such as eyes, nose, lips and chin, and so on.

Fingerprints—The patterns of ridges and valleys on the “friction ridge” surfaces of fingers—have been used in forensic applications for over a century. Friction ridges are formed in utero during fetal development, and even identical twins do not have the same fingerprints. The recognition performance of currently available fingerprint-based recognition systems using prints from multiple fingers is quite good.

Hand geometry—Hand geometry refers to the shape of the human hand, size of the palm and the lengths and widths of the fingers. Advantages to this modality are that is comparatively simple and easy to use.

Iris—The iris, the circular colored membrane surrounding the eye’s pupil, is complex enough to be useful for recognition. The performance of systems using this modality is promising.

Voice—Voice directly combines biological and behavioral characteristics. The sound an individual makes when speaking is based on physical aspects of the body (mouth, nose, lips, vocal cords, and so on) and can be affected by age,

emotional state, native language, and medical conditions. The quality of the recording device and ambient noise also influence recognition rates.

Signature—How a person signs his or her name typically changes over time. It can also be strongly influenced by context, including physical conditions and the emotional state of the signer. Extensive experience has also shown that signatures are relatively easy to forge.

Gait—Gait, the manner in which a person walks, has potential for human recognition at a distance and potentially, over an extended period of time.

Keystroke—Keystroke dynamics are a biometric trait that some hypothesize may be distinctive to individuals. Keystroke dynamics are strongly affected by context, such as the person's emotional state, his or her posture, type of keyboard, and so on (National Research Council of the National Academies, 2010, pp. 31–34).

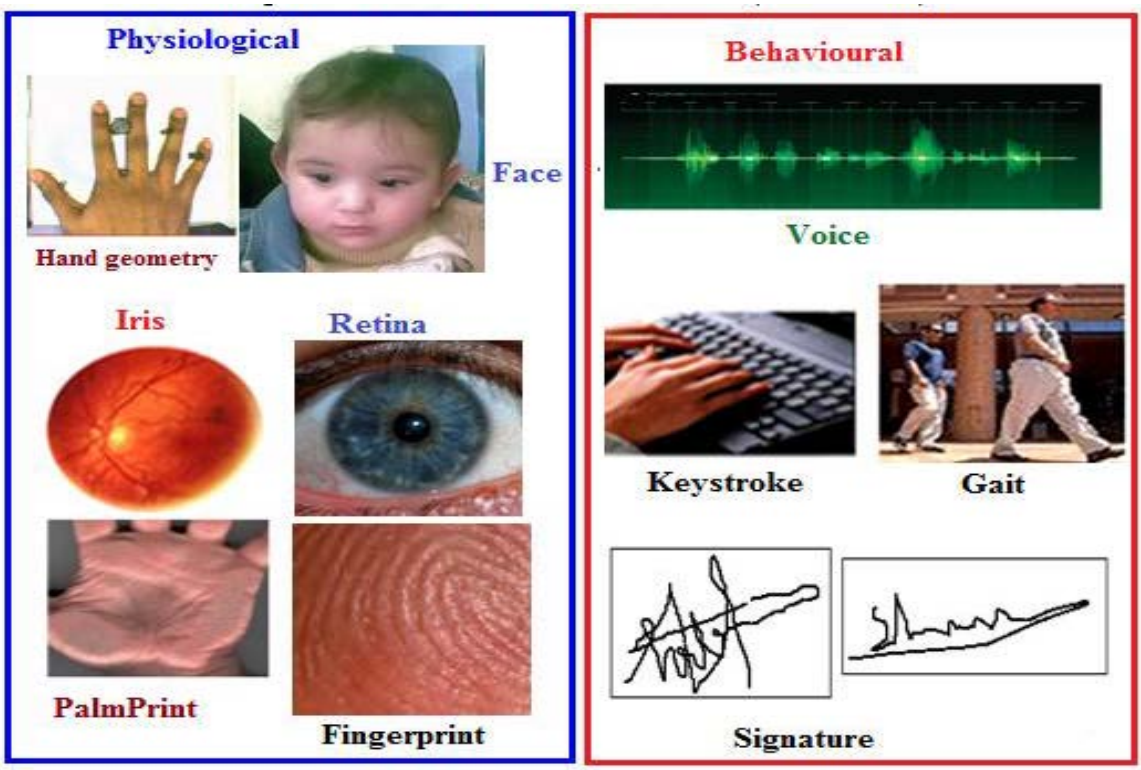

Figure 8. Biometric Modalities from AlMahafzah and AlRwashdeh, 2012

Biometrics as a process is an automated method of recognizing an individual. Biometrics is used in two ways: verification and identification. Verification compares one biometric to an identified biometric (1:1) to verify that an individual is who he says he is. Identification compares one biometric to a database of biometrics (1:N) to find out who an individual is (Center for Army Lessons Learned, 2011, p. 45).

When looking at the use of biometrics as a process, it is a process within a system. It cannot be stand-alone. Systems that perform biometric recognition exist within a constellation of other authentication and identification technologies and offer some distinct capabilities. Biometric technologies employ the last of these. Unlike password or token-based systems, biometric systems can function without active input, user cooperation, or knowledge that the recognition is taking place. One important difference between biometric and other authentication technologies, such as tokens, or passwords, is that these other technologies place trusts in cooperative users, allowing them to produce what they possess or demonstrate what they know (through dependence on the user's safekeeping of a token or password). These other forms of authentication do not protect against the sharing or transfer to the token or secret, whereas biometric traits are tied to an individual—specifically something an individual is or does (National Research Council of the National Academies, 2010, pp. 5–6).

2. Biometric Systems

Most biometric systems that are presently in use typically use a single biometric trait or single modality (unibiometric) to establish identity (Ross, 2007, p. 1). A recent trend in biometrics involves a shift from unibiometric to multibiometric systems. Unibiometric systems make use of a single source of biometric information to perform identity determinations (verification, identification, negative recognition, etc.). Both theoretical research and empirical observation of fielded systems reveal that single modal unibiometric systems are subject to a variety of shortfalls. Ceilings on performance accuracy, poor subject

population coverage, relatively high failure-to-enroll rates, and ease of circumvention are classic examples of such shortfalls (Bartlow and Zekster, 2009, p. 1). Some of the limitations of a unibiometric system can be addressed by designing a system that consolidates *multiple* sources of biometric information. This can be accomplished by fusing, for example, multiple traits of an individual or multiple feature extraction and matching algorithms operating on the same biometric.(Ross, 2007, p.1). Multi-biometric systems, which rely on more than one source of biometric input, can be used to alleviate such shortfalls. Arguably, such systems may also include other sources of information including biographic, travel document-based, etc.(Bartlow and Zekster, 2009, p.1).

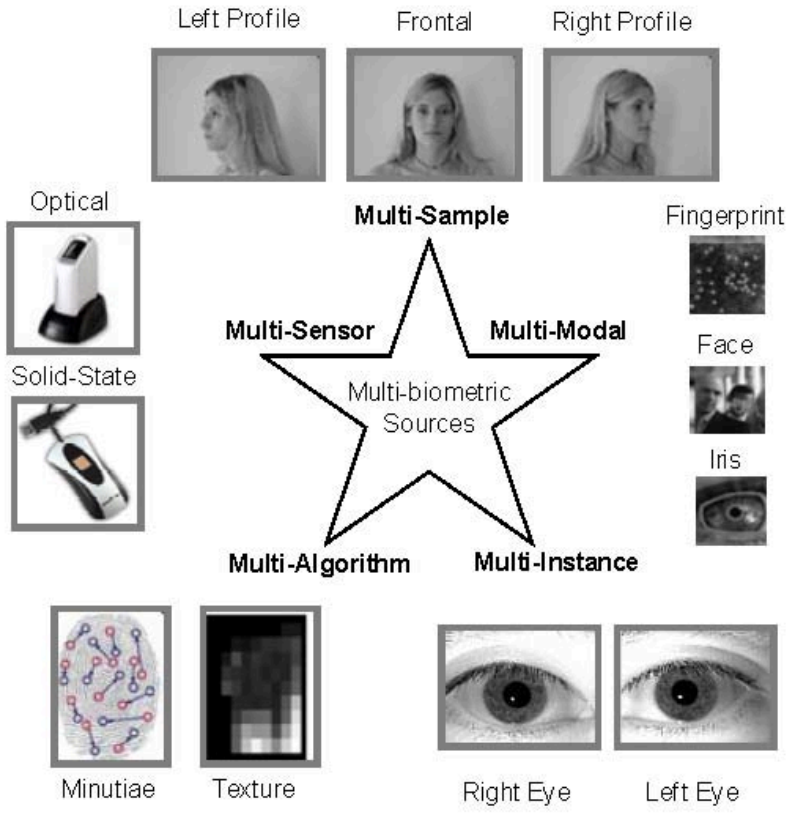

Figure 9. Multibiometric system from Bartlow and Zekster, 2009

There are numerous advantages to multibiometrics. Besides enhancing matching accuracy, the other advantages of multibiometric systems over traditional unibiometric systems are: 1. Multibiometric systems address the issue of non-universality (i.e., limited population coverage) encountered by unibiometric systems. 2. Multibiometric systems can facilitate the filtering or indexing of large-scale biometric databases. 3. It becomes increasingly difficult (if not impossible) for an imposter to spoof multiple biometric traits of a legitimately enrolled individual. 4. Multibiometric systems also effectively address the problem of noisy data. When the biometric signal acquired from a single trait is corrupted with noise, the availability of other (less noisy) traits may aid in the reliable determination of identity. 5. These systems also help in the *continuous* monitoring or tracking of an individual in situations when a single trait is not sufficient. 6. A multibiometric system may also be viewed as a fault tolerant system that continues to operate even when certain biometric sources become unreliable due to sensor or software malfunction, or deliberate user manipulation (Ross, 2007, p. 1).

3. Multibiometric Fusion

The utilization of biometrics in security systems is moving toward multibiometric systems. The newer multibiometric systems may be just as fast if not faster than the unibiometric system currently in place. “Many years of research have demonstrated that multibiometric fusion, the process of consolidating multiple sources of biometric information can significantly improve system accuracy over unibiometric systems.”(Bartlow and Zekster, 2009, p.2). Combining multiple sources of biometric sources has created a biometric fusion, which is the use of multibiometric inputs or methods of processing to improve performance. As stated, the traditional role of multibiometric fusion has been to increase system accuracy, increase the coverage across the population base, decrease instances of failures to acquire / failures to enroll, and increase the difficulty associated with circumvention. These four purposes directly relate to a subset of the characteristics typically used to evaluate a biometric modality. In

evaluating multibiometric modality systems, Jain and Ross, leaders in the biometric field, initially came up with the characteristics to evaluate biometric systems. The characteristics and parameters that are commonly utilized to evaluate a biometric system are:

1. Universality—Every individual accessing the application should possess a trait.

2. Uniqueness—The given trait should be sufficiently different across individuals comprising the population. How this modality separates individuals from other individuals.

3. Permanence—The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. How well the trait resists aging and fatigue over time. A trait that changes significantly over time is not a useful biometric.

4. Collectability—the ability to acquire and digitize the biometric traits using suitable devices and do not cause undue inconvenience to the individual. This is the ability to acquire and digitize the multiple biometric traits.

5. Performance—The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application. This includes speed, accuracy and robustness.

6. Acceptability—Individuals in the target population who will use the application should be willing to present their biometric trait to the system. Public acceptance.

7. Circumvention—This refers to the ease in which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits (Bartlow and Zekster, 2009, p.2).

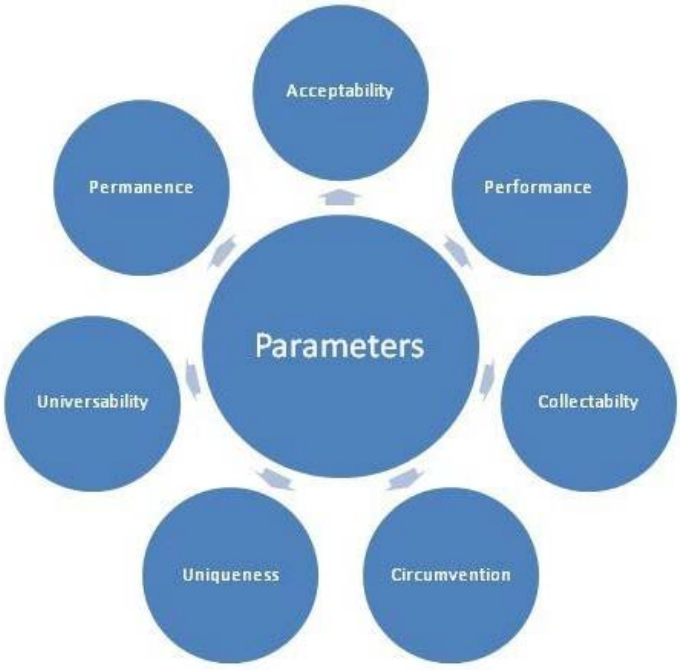

Figure 10. Parameter of Biometric Characteristics from Le, 2011

The objective in evaluating biometric systems and utilizing biometric fusion is to improve system accuracy, efficiency, applicability, and robustness. Some types of biometric fusion have been used successfully for years in large-scale fingerprint identification systems (Hicklin, Ulery and Watson, 2006, p.1). The trend toward multibiometric systems has been particularly prevalent in large-scale U.S. government systems such as Department of Defense Automated Biometric Identification System (DoD ABIS), Department of Homeland Security Automated Biometric Identification System (DHS IDENT), and FBI Next Generation Integrated Automated Fingerprint Identification System (IAFIS), all examples of multibiometric systems (FBI, 2012). The analysis of multiple traits (particularly related to performance) associated with multibiometric systems must come at the expense of increased processing time and computational complexity. However, through careful application of emerging technological advances, multi-biometric systems may not have such negative side effects (Bartlow and Zekster, 2009).

E. BIOMETRICALLY ENHANCED SECURITY DATABASES AND PROGRAMS

1. Governmental Biometric Databases

In the 19th century, identity management was much simpler and the individuals addressed identify concerns in an appropriate way for their time, today society is far more complex. Birth certificates, naturalization papers, passports, and other government issued documents prove citizenship, but are not enough with the sophistication of forgery in documentation. To augment these well-established and familiar tokens of citizenship, biometrics has emerged as a reasonable and effective way to identify individuals and prove who they say they are (National Science and Technology Council, 2011, p.5).

Government agencies have adopted biometrics for a variety of applications. For example, the criminal justice community, domestically and internationally, has been engaged in precursors to biometrics since the 1870's. In 1907, the Department of Justice (DOJ) established a Bureau of Criminal Identification, based upon fingerprints, and in 1924 charged the then-Bureau of Investigation with establishing a national identification and criminal history system that today is the Criminal Justice Information Services (CJIS) division of the FBI. CJIS operates the national criminal history and fingerprint based identification program using the Integrated Automated Fingerprint Identification System (IAFIS) (National Science and Technology Council, 2011, p.5).

Today, America's national security community uses biometrics to resolve and then anchor the identity of known and suspected terrorists (KSTs) by linking information independently collected and maintained by the Department of Defense (DoD); State Department (DoS); Department of Homeland Security's (DHS) - Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG); the Federal Bureau of Investigations (FBI) and state and local law enforcement partners. Biometrics, fingerprints and DNA forensic evidence, matched against an array of national biometric databases, allows identification and apprehension of KSTs, aliens,

criminals and others who would like to do us harm (National Science and Technology Council, 2011, p.3).

Interoperability in biometric programs is so vital that is was the subject of a June 2008 Presidential Directive, HSPD-24/NSPD-59, mandating that there can be no blockages or delays between the exchange of biometric and related information among key security agencies (BIMA, 2011, p.18). In the past decade, because of mandates and cooperation of numerous governmental agencies, advances have been made in the biometric technology in the government. The myriad of technical advances, interoperability remedies, sharing of information / data and the changes in the organization and peripheral cultural differences have allowed the current multibiometric capabilities, processes and systems to come into existence. Some of the major databases and programs that the government has because of this are described below.

a. Department of Justice (DOJ) – Integrated Automated Fingerprint Identification System (IAFIS).

The Integrated Automated Fingerprint Identification System (IAFIS) is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year, to help our local, state, and federal partners—and our own investigators—solve and prevent crime and catch criminals and KSTs. The IAFIS is a large database that provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints. The system not only stores fingerprints, but corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases. The system also includes civil fingerprints, mostly of individuals who have served or are serving in the U.S. military or have been or are employed by the Federal government. Additionally, state, local, and Federal law enforcement agencies submit fingerprints voluntarily. The IAFIS is the largest biometric database in the world. It processed more than 61 million fingerprint submissions during fiscal year 2010 and housed the fingerprints and criminal histories for more than 70

million subjects in the criminal master file, along with more than 31 million civil prints. Included in DOJ- FBIs criminal database are fingerprints from 73,000 KSTs processed by the U.S. or by international law enforcement agencies who work with the United States (FBI, n.d.). This biometric database includes biometric data from all military personnel and Federal employees. It also includes a majority of arrested individuals who have criminal records as well as latent fingerprints from crime scenes (Biometrics Task Force, 2010).

b. Department of Homeland Security (DHS) – Automated Biometric Identification System (IDENT).

The Department of Homeland Security (DHS) operates the Automated Biometric Identification System (IDENT). IDENT was originally developed in 1994 as a biometrics collection and processing system for the Immigration and Naturalization Service (INS). Since that time, the INS, as well as numerous other organizations, were subsumed and reorganized into DHS. This change has meant that the intended use of IDENT has expanded beyond that for which it was initially designed. This has necessitated a revision to the system of records notice (SORN). IDENT is the primary DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes. IDENT is primarily a biometric system that conducts identification or verification services on behalf of numerous U.S. Government programs that collect biometric and associated biographic data and is used for identification and verification services (U.S. Department of Homeland Security, 2006, p.2). IDENT maintains fingerprints, photographs and biographic information on more than 126 million individuals and conducts about 250,000 biometric transactions per day, averaging 10 seconds or less per transaction (National Science and Technology Council, 2011, p.5). The biometric data comes from visa applications, visitors entering the U.S., detainees from illegal border crossings and immigration violators (Biometrics Task Force, 2010).

c. Department of Defense (DoD), Biometrics Identity Management Agency (BIMA) – Automated Biometric Identification System (ABIS).

DoD-ABIS is a proven multimodal biometric system and database, that enables DoD agencies to conduct automated biometric searches 24 hours a day, 7 days a week and 365 days a year. The DoD-ABIS is the central repository and authoritative source for Defense Department multi-modal (face, fingerprint, iris and palm) biometric identity records for persons of interest. The network-centric system is accessible worldwide and interfaces with other U.S. government agency data systems. In 2011, the ABIS database had received almost 6.4 million submissions of biometrics data (BIMA, 2011, p.9). The majority of the biometric data that is stored within ABIS comes from biometrics taken from foreign nationals at overseas locations, who typically wish to gain access to U.S. installations, such as those in Iraq and Afghanistan. Information also comes from latent fingerprints, IEDs and other hostile actions, enemy combatants and detainees (Biometrics Task Force, 2010).

The Biometric Triad is comprised of three databases maintained by the DoD, DHS, and DOJ: the DoD Automated Biometric Identification System (ABIS), the DHS Automated Biometric Identification System (IDENT), and the DOJ/FBI Integrated Automated Fingerprint Identification System (IAFIS). The goal is to establish interoperability between the three databases. While the DOJ/FBI IAFIS is currently interoperable with DoD ABIS and DHS IDENT, DoD ABIS and DHS IDENT do not share mutual interoperability (Biometrics Task Force, 2010). The DoD ABIS already conducts fully automated data sharing with the FBI's IAFIS database. The controlling agency of the ABIS database, BIMA, is working toward the same level of interoperability with DHS' IDENT database, but has had difficulty coming to an agreement on the utilization and interfacing of the databases. The interoperability between the DoD ABIS and DHS IDENT represents the last remaining portion of the Biometrics Triad, per Homeland Security Presidential Directive (HSPD) 24's mandate for interagency biometric data sharing. While the DOJ/FBI IAFIS is currently interoperable with both DoD

ABIS and DHS IDENT, DoD ABIS and DHS IDENT do not share mutual interoperability. The DOS uses the DHS IDENT database for processing visa records and, when necessary, DoD and DHS share biometrics data and contextual information by loading biometric files onto a CD and hand-delivering the information to DHS for entry and storage in IDENT. The Biometrics Triad is working to bring an end to this slow and cumbersome work around procedure by setting the stage for automated interoperability, which will permit each database to share information with the other (Biometrics Task Force, 2010) The DoD ABIS already shares high-priority biometric datasets with key customers at DHS, such as Immigration and Customs Enforcement (ICE), Customs and Border Protection (CBP) and the U.S. Coast Guard (USCG) (BIMA, 2011, pp.18–20). In order for the U.S. government to have a fully integrated, robust biometric database system, the loop must be closed. After the loop is closed and procedures are placed, many other governmental agencies will be able to incorporate biometrics and interface with the Biometric Triad.

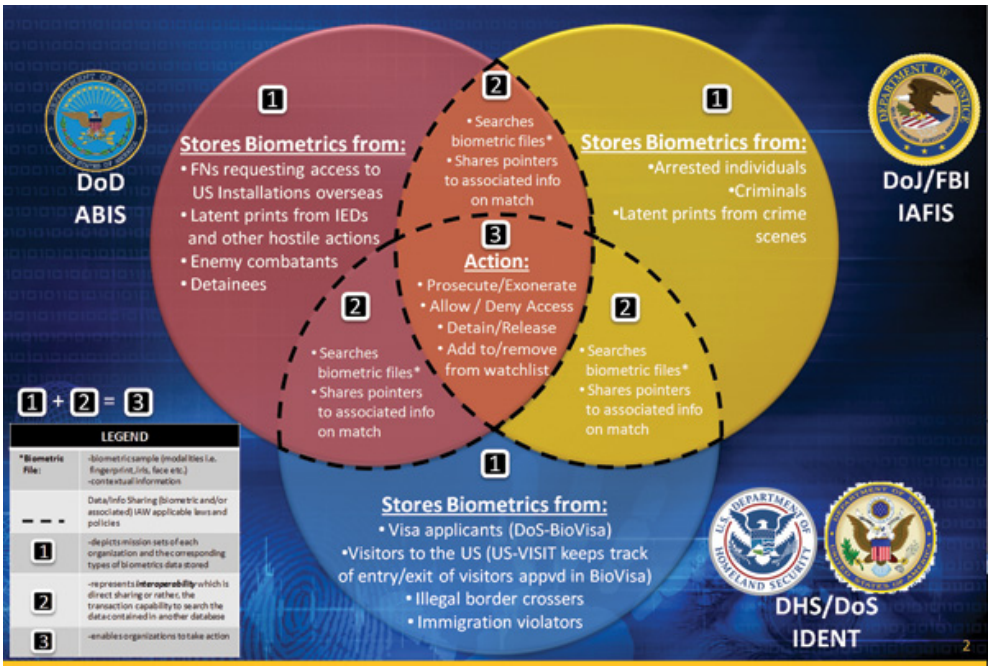

Figure 11. The Triad Desired end state from Biometrics Task Force, 2010

The United States has made great strides in trying to utilize biometrics as a way of identification. Within the past decade the United States has introduced some biometric programs that utilize three databases to identify individuals so they may gain access to the United States. These are the initial programs that illustrate the potential of biometrics and their use to verify identity and grant access. The three main programs in use are United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT), Global Entry (GE) and Transportation Worker Identification Credential (TWIC). Additionally the DOJ/FBI is developing the Next Generation Identification (NGI).

2. Governmental Biometric Programs

a. United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT)

The United States has more than 300 official ports of entry where nearly a half billion crossings occur every year. The Department of State (DOS) considers more than 9 million visa applications annually. DHS processes nearly 50,000 requests for asylum annually and processes approximately 30,000 applications for immigration benefits every day (National Science and Technology Council, 2008, p.28). The DHS' United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program provides biometric identification and analysis services to agencies throughout the immigration and border management, law enforcement, and intelligence communities to accurately identify people and assess whether or not they pose a risk to the United States. The U.S.-VISIT utilizes multibiometric system as its foundation because multiple traits are utilized and are unique, reliable, convenient and virtually impossible to forge. The U.S.-VISIT system uses the IDENT database provided by DHS. A complementary program from the Department of State (DoS) is BioVisa; a DoS program in which digital fingerprints and photographs like U.S.-VISIT are collected at U.S. visa-issuing posts around the world and stored in the IDENT database.

The most visible U.S.-VISIT feature is the collection and analysis of biometrics—digital fingerprints and a photograph from international visitors at U.S. visa-issuing posts (collection of biometrics is handled by the DoS BioVisa Program and U.S.-VISIT provides the analysis of the data against IDENT data base) The IDENT database provides U.S.-VISIT government agency customers with the information they need to make efficient and well informed decisions on the status of an individual. There are numerous benefits of biometric and the U.S.-VISIT program The U.S.-VISIT program establish and verify international visitors' identities for U.S. Customs and Border Protection (CBP) or DOS consular officers to help them make admission or visa-issuance decisions (National Science and Technology Council, 2008, p.29). The CBP utilizes U.S.-VISIT services at U.S. ports of entry to help facilitate legitimate travel, protect travelers against identity theft, prevent fraudulent document use, and keep our visitors and citizens safe from harm. The CBP officers are responsible for screening all international travelers to the United States. Using U.S.-VISIT services, officers quickly and accurately verify whether the person applying for entry is the same person to whom the visa was issued. And for all travelers, with or without a visa, officers use U.S.-VISIT services to verify that travelers are who they say they are and that they do not pose a threat to the United States (U.S. Department of Homeland Security, 2011).

The U.S. Citizenship and Immigration Services (CIS) uses the U.S.-VISIT program to help facilitate requests for immigration benefits. The U.S. Immigration and Customs Enforcement (ICE) officers receive credible leads on immigration violators through U.S.-VISIT. This enhanced information-sharing process provides an increased capability to identify and apprehend overstays which is a critical tool with which to manage the immigration and border system. Before U.S.-VISIT, international travelers who overstayed their authorized period of admission were only identified as a consequence of some other encounter with law enforcement (U.S. Department of Homeland Security, 2011). The U.S.-VISIT program establishes and verifies the identities of illegal migrants

apprehended by the U.S. Border Patrol (USBP) along U.S. land borders and the U.S. Coast Guard (USCG) at sea. The DoD uses biometric information about known or suspected terrorists on watch lists. The U.S.-VISIT program is working across the federal government to promote intelligence efforts in identifying high-risk persons and KSTs. The U.S.-VISIT biometric services also facilitate identification of terrorists by matching against latent fingerprints collected from terrorist safe houses and ongoing criminal investigations conducted around the world (U.S. Department of Homeland Security, 2011).

b. Transportation Worker Identification Credential (TWIC™)

Since 9/11, DHS has focused time and attention on enhancing the security of U.S. ports, particularly because of the role the ports play in the U.S. economy. Each day, $1.3 billion worth of goods move in and out of U.S. ports. In addition, many major urban centers (more than half to the U.S. population) and significant critical infrastructure are in proximity to U.S. ports or are accessible by waterways. As points of the entry and exit program, they are critical nodes that affect terrorist travel and transiting of material support or weapons. The economic, physical, and psychological damage that would result from a significant terrorist attack targeting maritime commerce or exploiting America's vulnerability at sea is difficult to estimate and a significant breakdown in the maritime transport system would affect the world economy (National Science and Technology Council, 2008, p.33).

The Transportation Worker Identification Credential (TWIC™) program is a Transportation Security Administration and U.S. Coast Guard initiative. The TWIC™ program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act, or MTSA, and all U.S. Coast Guard credentialed merchant mariners. An estimated 750,000 individuals require a TWIC™. To obtain a TWIC™, an individual must provide biographic and biometric information

such as fingerprints, sit for a digital photograph and successfully pass a security threat assessment conducted by TSA (U.S. Department of Homeland Security, 2011). A TWIC™ incorporates a customized computer chip containing a biometric identifier, a photograph, biographic information, four different digital certificates, and interfaces that can communicate in contact or contactless mode with a reading device. A port worker, longshoreman, or maritime worker of any nationality who's moving around at a U.S.-regulated port must have one (Homeland Security Defense Business Council, 2011, p.3–4).

TWIC™ uses biometrics for two primary identification purposes: background screening and verification. Background screening occurs prior to the issuance of a TWIC™ and encompasses an FBI criminal history records check and a check of DHS' IDENT database. Post-issuance, biometrics may be used at access control points to endure that the biometrics of the individual attempting to use the TWIC™ match those stored within the credential (National Science and Technology Council, 2008, p.34).

c. Global Entry (GE) Trusted Traveler Network

Global Entry is a program managed by U.S. Customs and Border Protection (CBP) that allows pre-approved, low-risk travelers expedited clearance upon arrival into the United States. Currently, only U.S. citizens and lawful permanent residents are eligible to join. Upon returning from international travel, Global Entry-enrolled travelers may bypass the regular passport control line and proceed directly to the Global Entry kiosk. The Global Entry process requires participants to present their machine-readable U.S. passport or permanent residency card, submit their fingerprints for biometric verification, and make a customs declaration at the kiosk's touch screen. The kiosk will compare the fingerprints presented to the fingerprints on file with the IDENT Database to confirm the traveler's identity. Upon successful completion of the Global Entry process at the kiosk, the traveler will be issued a transaction receipt and directed

to baggage claim and the exit unless chosen for a selective or random secondary referral (National Science and Technology Council, 2008, p.36).

d. Next Generation Identification – (NGI)

The events leading up to 9/11 showed these databases and searches were neither comprehensive enough nor rapid enough to support all counterterrorism challenges. Files have to be exchanged with DHS, DOS, and others to ensure that checks made by one department would not miss known or suspected terrorists (KST), persons with criminal backgrounds, etc. Biometric-based information also needed to be better coordinated among the intelligence community in order to "connect the dots." Additionally, every day, local, state, tribal, and Federal law enforcement agencies in the United States arrest more than 50,000 people and well over 60,000 people a day apply for positions of trust, visas to visit the United States, for citizenship, etc. (National Science and Technology Council, 2008, p.37). In each case, a check has to be made to determine if there are any facts that would make them unsuitable or indicate that they may not be trusted. The FBI meets these identification challenges through electronic processing of fingerprint-based background checks by its CJIS Division using the Integrated Automated Fingerprint Identification System (IAFIS).

Driven by advances in technology, customer requirements, and growing demand for Integrated Automated Fingerprint Identification System (IAFIS) services, the FBI has initiated the Next Generation Identification (NGI) program. This program will further advance the FBI's biometric identification services, providing an incremental replacement of current IAFIS technical capabilities, while introducing new functionality. The NGI system will offer state-of-the-art biometric identification services and provide a flexible framework of core capabilities that will serve as a platform for multimodal functionality. The future of identification systems is currently progressing beyond the dependency of a unimodal (e.g., fingerprint) biometric identifier towards multimodal biometrics

(i.e., voice, iris, facial, etc.). The NGI Program will advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multimodal system that will facilitate biometric fusion identification techniques. The framework will be expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems. Once developed and implemented, the NGI initiatives and multimodal functionality will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification (FBI, n.d.).

F. SUMMARY AND CONCLUSION

The current aviation security passenger-screening program has been a program of "one size fits all" since the tragic events of 9/11. This program has impacted the way United States citizens travel, which has had an effect on the economy of the United States. A trusted traveler program should be implemented in the United States. This trusted traveler aviation security passenger-screening program should use risk management as its foundation. The basic logic of the trusted traveler program is to reallocate security resources from those "low-risk" travelers and devote them to the unknown risk population.

The literature has differing opinions on the key elements that should be included for the trusted traveler program. It is agreed the program should be voluntary, include a thorough background check and reduce resources needed. Where the opinions differ; however, is how to implement the program. While adopting a common trusted traveler aviation security passenger-screening program would have many potential benefits, the literature lacks specific details that could affect implementation. This appears to be a gap within the literature.

The literature indicates a risk-based security framework for aviation passenger screening has been adopted by the TSA for many different exploratory pilot programs in 2011. By adopting these risk-based methodologies, the TSA is improving checkpoint efficiency while decreasing aviation passenger

wait times and providing tax savings to the U.S. taxpayer. These programs have had success, but critical examination through literature shows that these programs do not incorporate a mechanism for positive identity authentication; they only utilize identity documentation for authentication.

A current challenge of the current RBS initiative is it does not incorporate biometric identification validation into the process. The TSA as an agency continues to only utilize documentation to validate passenger entry into the secure passenger screening area. A way to improve entry into the secure passenger screening area is to incorporate a biometric validation process and a risk-based “Trusted Traveler” program, while expediting and enhancing the low-risk passenger traveling experience. Truly legitimate passenger security requires positive identification authentication of trusted travelers to be able to differentiate between the “trusted traveler” and those who mean to do us harm. This RBS initiative will assist the TSA by concentrating their limited resources on a very small percentage of passengers who are unknown or have indicators of doing harm from validated trusted travelers.

Technology has made monumental advances in the past ten years in the automated recognition of individuals based on biological and behavioral characteristics. There has been increased eagerness to utilize biometrics because it increases convenience and efficiency for routine access, validates an individual’s identification, and reduces fraud while enhancing public safety and security. Biometrics have been incorporated into systems and have utilized a single biometric trait or single modality system up until the past few years. The literature illustrates the new trend for biometric systems is to employ multibiometric traits or multimodal systems that utilize multiple biometric sources to create a biometric “fusion” that significantly improves system accuracy. Until recently, the nexus of biometrics and the way they have been evaluated has been inconsistent. Adopting common evaluation characteristic criteria for biometric systems will assist with evaluating and improving, while providing a common benchmark for implementation.

The United States government in the past decade has adopted, on a large scale, biometrically enhanced security programs. The advent of these programs has shown there is an inconsistency in sharing standards and a stove piping of information based on departments. The literature suggests they are trying to bridge the gap between these databases and programs and are creating a "biometric triad" that fully integrates the government's three main databases and programs. The majority of large governments and agencies are adopting and incorporating biometrics as their identification standard. The adoption of biometrics is increasing the efficiency, accuracy and reliability of services and processes in the validation of identification for their internal programs.

A gap that has been found is biometrics have not been incorporated into all departments and agencies that have a service of identity verification role for national security and public safety. Currently, the TSA does not use biometrics in their RBS APSP program and serious consideration should be given because of the vital role it has in our national security and economy.

The TSA will continue the struggle to maintain a balance between carefully screening passengers and crewmembers while avoiding undue delays to the traveling public. Further study and research in the utilization of biometrics into a risk-based screening process could make for a better passenger screening system. The TSA will never be able to function as a truly risk-based organization until the agency can differentiate between a passenger's identity-based on every level of risk. The TSA must develop an expedited screening program using biometric credentials that would allow the TSA to positively identify trusted passengers and crewmembers, so the agency can prioritize its screening resources on individuals of high risk while speeding up the screening process (Peterman, Elias and Frittelli, 2011, p.5).

III. RESEARCH METHOD

A. APPROACH

The research was conducted in four steps:

1. Analyze Risk-Based Security-- Analyze the TSA RBS initiatives currently being incorporated into the aviation passenger-screening model. Analysis of three RBS initiatives (KCM, DoD CAC, and TSA Pre✓™) will review strengths, limitations and gaps in security efficiency and reliability.

2. Identify Current Biometric Technologies-- Identify current biometric technologies that exist today and are commercially available, that can be incorporated to improve passenger identity authentication. Current biometric characteristic (i.e., iris, facial recognition, fingerprint) technologies utilized in biometric systems for improving efficiency, reliability and precision in common practices and day-to-day activities will be examined to discover strengths and limitations.

3. Analyze Biometrically Enhanced Security Programs-- Discover the strengths and limitations of other successful biometrically enhanced security programs, both governmental and non-governmental. Discover the strengths, limitations and gaps in security efficiency and reliability of these programs.

4. Integrate Biometric Technologies into a Risk-Based Security Program Model—Explore improving the current RBS aviation passenger screening model by incorporating biometric security enhancements discovered in earlier phases of this research to improve efficiency and reliability. Recommendations will be applied to the current model by incorporating biometric technology into the current model to create a feasible and ideal RBS aviation passenger-screening checkpoint that incorporates biometrically enhanced security measures.

B. DATA SAMPLE FOR ANALYSIS

The research steps are discussed in detail below.

1. Analyze Risk-Based Security

The data sample for analyzing Risk-Based Security (RBS) was compiled and derived from the current TSA RBS Initiatives: KCM, Secure Flight, TSA Pre✓™ programs. The data came from TSA documentation (websites, studies, agency literature). The data analysis of the RBS initiatives attempted to find the strengths, limitations and gaps in security that exist in the current aviation passenger-screening model. The analysis aimed to show the security limitations and potential security gaps at checkpoints. It identified where biometric security enhancement measures can possibly be incorporated to bridge and address the limitations of the identified security checkpoint gaps.

2. Identify Current Biometric Technologies

The data sample for identifying biometric characteristic technologies was material published by leading researchers, the federal government's biometric agencies and leading commercial enterprises. The data was collected from resources such as:

- The Biometric Consortium (biometrics.org), which is the focal point for research, development, testing evaluation, and application of biometric-based personal identification/verification technology,
- Biometrics.gov, the central source of information on biometrics-related activities of the Federal government, and
- The FBI Biometric Center of Excellence (BCOE), the leading government program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for integration into operations.

Interviews were conducted of senior policymaking leadership in order to gain insight and emerging technology to try to discover technology that can be

fielded within the next 18–24 months to better enhance security at aviation security checkpoints. This information is not readily available in written documentation because much of the technology is new and rapidly developing; there is a revolution in biometric technology security enhancements and new enhancements are being discovered every day. The interviews were conducted to capture the gaps that may exist in the literature. Individuals from the following organizations were interviewed:

- Department of Justice/Federal Bureau of Investigation's Biometrics Center of Excellence (BCOE). BCOE is it is the FBI's program for exploring and advancing the use of new and enhanced biometric technologies and capabilities for the integration into operations. BCOE focuses its efforts on fostering collaboration, improving information sharing and advancing the adoption of identity management solutions within the FBI across national security communities.
- Department of Homeland Security Automated Biometric Identification System (IDENT) is a DHS-wide system for the storage and processing of biometric and limited biographic information of DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions, and to provide associated testing, training, management reporting, planning and analysis, or other administrative uses.
- Department of Defense Biometric Identity Management Agency (BIMA). BIMA was chosen because it is a premier organization dedicated to protecting the nation through the employment of biometric capabilities and is DoD's lead program to coordinate, integrate, and synchronize biometric technologies and capabilities in support of national security.
- FST21 Ltd. The Corporation FST21 Ltd. was chosen because it is an award winning biometric corporation that designs identity-based solutions using next-generation biometric technology for providing security. This non-government corporation is utilizing facial and voice recognition as a key component to its biometric solutions.

During these interviews no personally identifiable information (PII) or personal health information PHI (PHI) was collected. The analysis attempted to discover the strengths and limitations of current biometric characteristics

technology. The outcome of the analysis was to identify promising biometric characteristic technology available in terms of efficiency (cost, speed and practicality), reliability (low failure rate) and anticipated utilization for integration into the RBS initiatives for aviation passenger screening. Not every biometric company or organization was researched or interviewed; only some companies/organizations that have promising technologies available for TSA to leverage.

3. Biometrically Enhanced Security Programs

The data sample for examining other biometrically enhanced security programs was government and non-government commercial enterprises utilizing biometrically enhanced security measures in their security. The analysis focused on successful uses and strengths of biometric technology in government departments and agencies, as well as non-government commercial enterprises. A review of the following programs was conducted:

- DOJ/FBI's IAFIS program
- DHS's IDENT program
- DoD's BIMA ABIS databases
- United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT)
- Transportation Worker Identification Credential (TWIC) and
- Global Entry (GE) programs

These programs have been on the forefront of incorporating biometrically enhanced security measures into government programs. Through inquiry of these programs, the data analysis sought to discover insight into possible biometrically enhanced security measures that can be incorporated or modeled after for improving RBS initiatives into the aviation passenger-screening model.

4. Integrate Biometric Technologies into a Risk-Based Security Program

This section of the thesis will integrate biometric technologies into the risk-based security programs and the current aviation passenger-screening model. Process Modeling of the current RBS initiatives program to incorporate biometric security enhancements discovered in the earlier steps of this research will attempt to show how to improve the efficiency and reliability of the aviation passenger-screening design. The anticipated outcome of the program evaluation and inquiry will be to discover, envision, design, and create an unrealized possibility for an improved RBS initiatives aviation passenger-screening model. The goal will be to seek the amalgamation of all or some of these biometric technologies into the RBS initiatives aviation passenger-screening model to create an improved security checkpoint at all U.S. federalized airports improving security efficiency and reliability and decreasing the cost of the current model.

C. SUMMARY

Modeling the current RBS initiatives programs to incorporate biometric security enhancements discovered in the analysis and research from this study explores how to improve the efficiency and reliability of the aviation passenger-screening design. The anticipated outcome of the program evaluation and inquiry were to discover, envision, design, and create an unrealized possibility for an improved RBS initiatives aviation passenger-screening model. The findings from the program evaluation, research and inquiry incorporated the best practices and most promising concepts and illustrate by integration what advantages they would bring to the current RBS initiatives aviation passenger-screening program. The goal of the thesis is to seek the amalgamation of all or some of these biometric technologies into the RBS initiatives aviation passenger-screening program to create an improved security checkpoint at all U.S. federalized airports improving security efficiency and reliability and decreasing the cost of the current model.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS

A. INTRODUCTION

This chapter conducts analysis that follows the method contained in Chapter III. Using literature on the TSA's RBS program, the first step analyzed three of the six current RBS initiative programs that have the greatest potential for incorporating biometric technology to enhance security. The programs that have the greatest potential for integrating biometric technology are: TSA Pre✓™ DoD's CAC and KCM. The analysis shows a detailed overview of possible vulnerabilities within the current systems. The next step examined the current biometric technologies that were the most favorable to be utilized in providing security enhancement for the TSA RBS initiatives. The data was collected from U.S. Government documents, reports, news media, scholarly works and interviews of senior policy makers. The last step in this analysis chapter was to analyze U.S. Government biometrically enhanced security programs and commercial biometric capabilities. The programs examined were DHS's United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program, TSA's Transportation Worker Identification Credential (TWIC) program, CBP's Global Entry (GE) program, and DOJ/FBI's Next Generation Identification – (NGI) which is an emerging future program. The data collected was from reports, scholarly works and interviews. Cumulatively the analysis was utilized to make a recommendation for how to improve the current RBS initiative programs and make an ideal, near-future biometrically enhanced security checkpoint. The analysis provides a holistic view on how the TSA can better the RBS initiatives while improving the Aviation Passenger-Screening Program and procedures with biometrics.

B. OPPORTUNITY FOR CHANGE

Incorporating biometric technology into the current Risk Based Security Initiatives aviation passenger-screening program can improve effectiveness of

airport security checkpoints by reducing the long wait times and reducing the length of the lines. The incorporation of biometric technology would improve the efficiency and effectiveness of the checkpoints by more rapidly validating an individual's identification, determining the trustworthiness level of the passenger or "trusted traveler"; in turn this will lessen the requirements and level of scrutiny for checkpoint screening.

In a trusted traveler program, upon reaching a position in a separate security line for just trusted traveler enrollees, the traveler would present biometric information to a TSA managed biometric collection device. Upon biometric validation of the individual's identification as a trusted traveler, the traveler would pass through special security checkpoints without divesting personal items in pockets and would leave external garments and shoes on. Separately, carry-on bags would be x-rayed and scrutinized for certain dangerous items not to be brought onto the aircraft (U.S. Travel Association n.d. pp.13–14). The efficiency and effectiveness of the checkpoints would increase because of reduced item removal and divesting burden requirements. Wait times would lessen because of the improved procedure and lines would decrease by validating trustworthy passengers who would need fewer inspections and scrutiny at security checkpoints since they are a low risk or threat to the aviation enterprise. This new approach greatly increases risk mitigation from the current approach utilized today.

C. RBS INITIATIVE PROGRAMS ANALYSIS

1. TSA Pre✓™

The purpose of TSA Pre✓™ is to have expedited security screening based on risk category. Under TSA Pre✓™ individuals provide information about themselves prior to flying in order to potentially expedite their screening process and travel experience. By learning about travelers through the information they voluntarily provide, the TSA can classify passengers into one of three risk categories; low-risk: passengers who have been subjected to a

background check, have been vetted and deemed to be a trusted traveler; unknown: passengers the TSA does not have enough information on to deem them low or high-risk and have not been vetted; and high-risk: passengers who are on watch lists, selectee lists and no-fly lists and pose a possible danger to other passengers. This is conducted through Secure Flight, which is a TSA program that matches passenger information to government watch lists. Secure Flight begins 72 hours prior to, up to just hours prior to a passenger's flight by confirming a person's identity, reviewing the boarding pass. This vetting allows a passenger to be placed into a category. Those low-risk passengers are allowed to enter into the TSA Pre✓™ lane for expedited screening. In the TSA Pre✓™ lane, passengers do not have to remove their shoes or belts, divest items from pockets and they are allowed to wear a light jacket as they process through the lane. Additionally, passengers no longer have to remove laptops or liquids, aerosols or gels less than 3.4 ounces from their carry-on baggage. This greatly lessens the wait time at security checkpoints where most passengers are passing through security checkpoints in less than one minute. With fewer screening requirements, the TSA can adjust its resources both on equipment and personnel to focus on high-risk passengers. Currently there are two ways an individual can be enrolled into the new TSA Pre✓™ program. One is by joining CBP's Global Entry program. Which is a biometrically enhanced security program for international travelers returning to the United States. In order to join this program one must be a U.S. citizen, undergo an extensive background check vetting including criminal and terrorist background checks followed by a sit down interview with a uniformed Customs and Border Protection Law Enforcement Officer (LEO). During the interview a 2D biometric facial photograph is taken and 10-point fingerprints are taken as well creating a reference biometric in the database. Additionally, there is a $100 enrollment fee that is good for five years and the program is voluntary. The individual must meet all requirements in order to be enrolled. By having a Global Entry card you are authorized to utilize the TSA Pre✓™ lane. Another way to be enrolled in the TSA Pre✓™ lane is by

being a U.S. citizen that is a member of participating airline upper tier frequent flyer programs who has met the requirements for significant flown mileage/segment totals for eligibility. Additionally, the individual may be subject to an intelligence risk-assessment conducted by TSA. Furthermore, selection is recommended by the airline and the individual must voluntarily submit to the requirements of the program.

TSA Pre✓™ has been in existence since late 2011 and in essence is an airline based program designed to be used by premier passengers and is not available to the larger pool of passengers who may be eligible to use the TSA Pre✓™ lanes. TSA has stated their goal is to have 70% of passengers enrolled, but currently has less than 10% of passengers enrolled in the program. The main reason sited is pre-check eligibility is complicated due to confusing rules from airline to airline and can frustrate passengers. Additionally, the process for notifying passengers is not clear and even if the passenger is eligible, the passenger can only use the pre-check on the carrier that offered them the enrollment into pre-check in the first place (Crosby, 2012, pp.23–24).

The analysis of this program shows it is not standardized in how enrollment is conducted, who is eligible for the program, how the vetting process is directed, and who is in control of the process. There is insufficient consistency in the background checks. For example, some are enrolled simply based on the frequency of their travel with no verification of their true identity. Other individuals must go through an entire governmental criminal/terrorist background check and voluntarily submitting their biometrics for enrollment.

2. DoD's CAC

Active duty members of the Army, Navy, Air Force, Marine Corps, Coast Guard, as well as active duty members of the National Guard and Reserve, who are issued Common Access Cards (CAC) by their departments are eligible to participate in the TSA Pre✓™ lanes (Transportation Security Administration, 2012). DoD CACs are smart cards the size of a credit card and are standard

identification for members of the Uniformed Services, Selected Reserve, DoD civilian employees, and eligible contractor personnel. This is the principle card used to gain access to military installations, buildings and computer networks and systems. The card contains a computer chip, which holds name, gender, benefits and privileges information, blood type and organ donor information (military only), digital certificates and other application-specific data. The card also contains an updateable magnetic strip used for building access information as well as a barcode containing name, SSN, DOB, personnel category, pay category, benefits information, organizational affiliation and pay grade. Biometric data is stored on these cards as well (www.dmdc.osd.mil/smartcard, 2012). Individuals who possess a DoD CAC may enter the TSA Pre✓™ lanes for expedited screening and do not to be in uniform.

Analysis of this program under TSA Pre✓™ shows numerous individuals may obtain DoD CACs including contractors and non-U.S. citizens which creates a possible security gap where a non-eligible individual could circumvent the system and gain access. Additionally, some of these CACs are still retained after service members leave active duty service or retire. This makes them ineligible, but they can still access the TSA Pre✓ lanes with the card in their possession. In the future, the long-term vision is that TSA's Secure Flight and DoD will partner to identify and verify DoD personnel prior to being able to use the TSA Pre✓™ lane. Currently, the option to automatically be enrolled and code their boarding passes for TSA Pre✓™ does not exist. It must be done manually. Active duty personnel present their CAC and boarding pass to the document checker in the TSA Pre✓™ lane who then will scan the CAC to verify the status of the Active Duty member with the DoD. This program has had issues in the preliminary stages with connectivity and equipment.

3. KCM

Know Crew Member is a joint partnership effort with Airlines for America. The Air Line Pilots Association, and TSA that allows uniformed flight deck crew

members (airline pilots and flight attendants) expedited access into the sterile area through exit lanes, checkpoints and common access areas. The crewmembers no longer go through aviation passenger-screening checkpoints and no longer go through traditional screening processes. Crewmembers merely show their airline credentials with photograph at one of the KCM access points that has a CrewPASS™ access management workstation. This workstation is utilized by a TSO to validate the identity and privilege status of each airline crewmember. When using CrewPASS, each uniformed crewmember will present the TSO with their airline badge containing their photograph, airline name, and employee ID number. The crewmember's employee ID number, airline employer and fingerprint are forwarded via encrypted link to the ARINC CrewPASS Server. This service is located in ARINC's secure computer facility (a privately owned facility) in Annapolis, Maryland.

The CrewPASS access process provides an expedited screening process for U.S. commercial airline crewmembers. In fact, no screening is accomplished at all. If the employee ID matches the query to the CrewPASS Server the crewmember is granted access to the sterile area bypassing the traditional screening process.

Analysis of this program shows the CrewPASS architecture has the potential to provide both an employee verification and biometric component, but the biometric portion has not yet been implemented (Ryan, 2010, pp. 1–4). The current CrewPASS architecture utilizes former Cockpit Access Security System (CASS) to create a separate CrewPASS system and database. The entries into the database are performed and maintained by the airlines themselves. Effectively, the database verifies whether the crewmember is still employed by the airline and is still in good standing when the query is made at the CrewPASS workstation by the TSO. The security gap here is the database is maintained by the airlines and absent the biometric portion of the system, the identity of the crewmember cannot be verified.

4. Summary of RBS Initiative

Analysis of the RBS initiatives programs showed there are numerous low-risk trusted travelers who can go through expedited screening processes to reduce the burden on the exponentially growing passenger loads and travel experience. There are numerous databases and systems being used to vet eligible low-risk travelers. The fundamental security gap that everything points to is there is not a process to verify the identity of any of these trusted travelers. There is no standardization in the classification, vetting, validating and entering them into the low-risk population. Furthermore, some of the systems have the potential to incorporate biometrics into the pre-screening and screening process, yet to date have not been utilized for verification of these potential low-risk travelers. This creates a less then optimal alternate aviation passenger-screening system.

D. ANALYSIS OF CURRENT BIOMETRIC TECHNOLOGIES (MODALITIES)

A biometric modality refers to a system built to recognize a particular biometric trait. Face, fingerprint, hand geometry, palm print, and iris are all examples of biometric traits. Biometric systems are not modality specific but have major implications for system design and performance (Whither Biometrics Committee, 2010, pp.31–32). Biometrics are used for many different purposes. They are either part of a biometric verification system or an identification system. The verification system seeks to answer the question, “Is this person who s/he says s/he is?” The system checks his/her biometrics sensor scan such as face, fingerprint or iris against the baseline biometric digital template in the database file. Verification systems are 1:1 matching systems because the system matches the biometric presented by the individual against a biometric already on file. This type of system is usually faster and more accurate than identification systems even when the size of the database increases. On the other hand, identification systems seek to identify an unknown person or his/her unknown biometric. They try to answer the question, “Who is this person?” Identification systems try to

check biometrics presented against all others already in the database. These are described as a 1:n system where n is the total number of biometrics in the database. An example of this is where a latent fingerprint is picked up at a crime scene and an attempt is made to identify that unknown person by that biometric trait (Lynch, 2010, pp. 4–6).

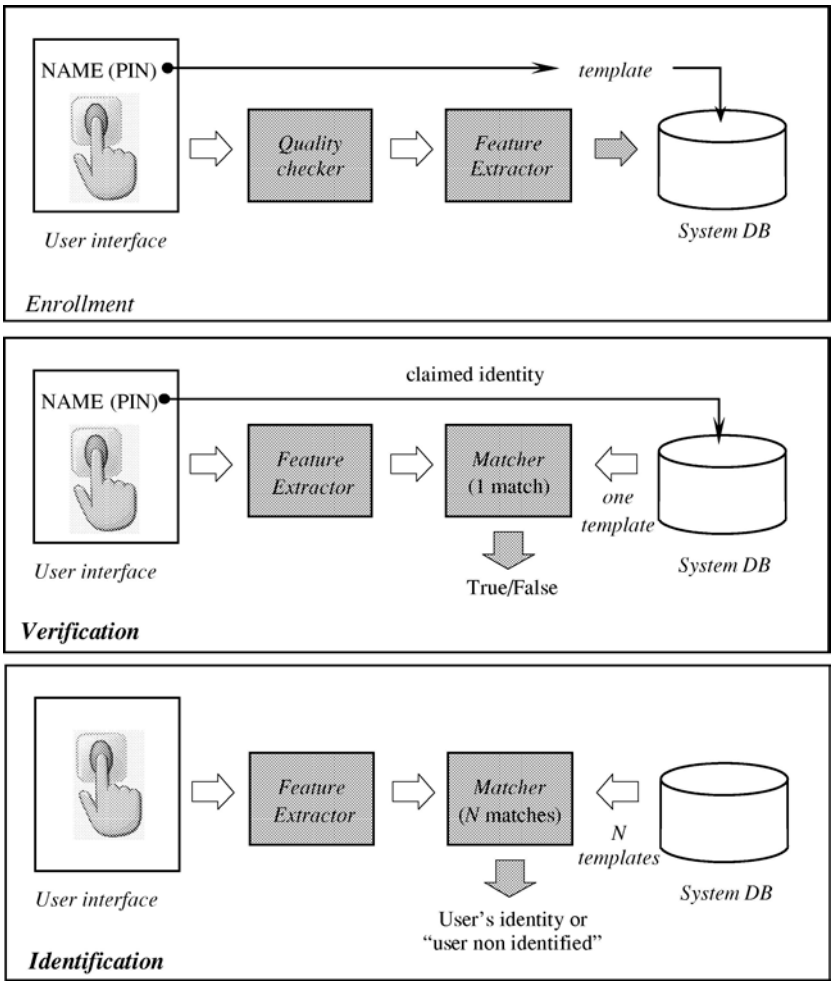

Figure 12. Diagrams of enrollment, verification, and identification tasks from Jain and Ross, 2004

While researching next generation identity verification it was discovered that person authentication using fingerprint or voice biometrics traits has increasingly been deployed for day-to-day security and surveillance applications. As outlined, one of the most acceptable non-intrusive physical attributes to authenticate and verify is the face. In one study, next generation identity

verification based on face/gait biometrics, they conducted a comparison of various biometric technologies against the standard biometric criteria established by Jain, one of the predominant biometric experts in the field. From the report the choice of a particular human characteristic to be used as a biometric trait depends on the following criteria:

- **Uniqueness** is how well the biometric separates individually from another
- **Permanence** measures how well a biometric resists aging.
- **Collectability** ease of acquisition for measurement.
- **Performance** accuracy, speed, and robustness of technology used.
- **Acceptability** degree of approval of a technology.
- **Circumvention** ease of use of a substitute

From the study a table was created that shows a comparison of existing biometric systems in terms of the above criteria. From the comparison of various biometric technologies according to AK Jain, face, fingerprint, iris and DNA were the highest performing modalities for identification verification through biometrics (Hossain and Chetty, 2011, pp.142–144).

Comparison of vaious biometric technologies, according to A.K. Jain (H=High, M=Medium, L=Low)
Circumventability listed with reversed colors becasue low is desirable here instead of high

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystrokes	L	L	L	M	L	M	M
Hand Veins	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retinal Scan	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermograph	H	H	L	H	M	H	H
Odor	H	H	H	L	L	M	L
DNA	H	H	H	L	H	L	L
Gait	M	L	L	H	L	H	M
Ear Canal	M	M	H	M	M	H	M

Table 1. Biometric Technology Comparison Table from Jain, 2004

Additionally, interviews with senior policy makers in the biometric field validated the findings that fingerprints, face and iris are the highest performing modalities for identity verification using biometrics. Because of this, it was decided to focus on these three modalities as the most promising for implementation into the RBS Aviation Passenger-Screening Program; facial recognition, fingerprint recognition and iris recognition. These three were selected based on research conducted by the National Science and Technology Council, National Research Council of the National Academies and interviews with senior policy makers and academicians in the biometric field who recommended these three as being the best for incorporating into a biometric verification system. There is universal consensus that not one biometric modality is best for all implementations and the more modalities utilized in verification the better the probability of positive identity verification.

1. Facial Recognition

The human face plays an irreplaceable role in biometrics technology due to some of its unique characteristics. First, most cameras are non-invasive; therefore face verification systems are one of the most publicly acceptable verification technologies in use. Another advantage is that face detection

systems can work mostly without the cooperation of the user concerned, which is therefore very convenient for the general user (Kumar and Srinivasan, 2012, p.43). Face recognition is a non-intrusive method, and facial attributes are probably the most common biometric features used by humans to recognize one another. The applications of facial recognition range from a static, controlled "mug-shot" authentication to a dynamic, uncontrolled face identification in a cluttered background (Ross, Nandakumar and Jain, 2006, p.21). Humans recognize familiar faces with considerable ease, but they have difficulty recognizing unfamiliar individuals. Since the 1960's machine vision, researchers have been developing automated methods for recognizing individuals via their facial characteristics. Despite the volumes of research, there are no agreed-upon methods for automated face recognition such as there are for fingerprints, but they are rapidly reaching a consensus that 3D imaging will be the standard. Multiple approaches have existed for several years using low-resolution 2D images. Recent work in high-resolution 2D and 3D show the potential to greatly improve face recognition accuracy (National Science and Technology Council, n.d. p.81). Furthermore, there has been rapid development of 3D image technology. Using 3D image technology has become another alternative in the field of biometrics. 3D facial templates record the exact geometry of a person and are irrelevant with respect to the illumination changes of the environment or the orientation changes of the person (Li and Barreto, 2005, p. 1). However, there has been significant progress in improving the performance of computer-based face recognition algorithms over the last decade. It was discovered that computer face recognition using algorithms now surpasses the human ability to recognize a face. In other words, computers have become more accurate at recognizing human faces, even more so than humans themselves (O'Toole, Phillips, Jiang et al., 2006, p.1). In other studies it has been found 3D face recognition and identification have definite advantages; some of which are: face recognition is a modality that humans largely depend on to authenticate other humans; face recognition is a modality that requires no or only weak cooperation

to be useful; face authentication can be advantageously included in multimodal systems, not only for authentication purposes but also to confirm the aliveness of the signal source of fingerprints, iris, etc. (Li and Barreto, 2005, p.2) The future of biometric technology is demonstrating that facial recognition will be at the forefront of biometrics for many years to come and may someday replace the centuries old system of using fingerprints.

Figure 13. Illustration of Facial Recognition from fbi.gov

2. Fingerprint Recognition

Fingerprint recognition is by far the most well known and the oldest biometric modality that is in use today. Humans have used fingerprints for personal identification for centuries dating back to the Chinese in the 14th Century. The matching (i.e., identification) accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of fetal development (Ross, Nandakumar and Jain, 2006, p.21). Manual comparison of fingerprints for recognition has been in use for many years, and

has become an automated biometric identification technique over the past two decades. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial image through live scan of the finger by direct contact with a reader device. The feature extraction module to compute the feature values uses images acquired by the sensors. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template (Kumar and Srinivasan, 2012, p.41). A major problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Lastly, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, ageing, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing) or digits may even be missing (Ross, Nandakumar and Jain, 2006). Despite technological hindrances fingerprints are still the most widely accepted biometric trait since fingerprint templates have been created and stored for over a hundred years.

Figure 14. Illustration of Digital Fingerprinting from escanfingerprinting.ca

3. Iris recognition

The iris is the colored portion of an individual's eye. To obtain a good image of the iris, identification systems typically illuminate the iris with near-infrared light, which can be observed by most cameras yet is not detectable by, nor can it cause injury to, humans. A common misconception is that iris recognition shines a laser on the eye to "scan" it. This is incorrect and untrue. Iris recognition simply takes an illuminated picture of the iris without causing any discomfort to the individual (National Science and Technology Council, n.d. p.81). The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and support the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and even the irises of identical twins are different. It is possible to detect contact lenses printed with a fake iris. The hippus movement of the eye may also be used as a measure of liveness for this biometric. Although early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective (Ross, Nandakumar

and Jain, 2006, p.23). Iris recognition is the best breed authentication process available today. Iris recognition takes a picture of the iris; this picture is used solely for authentication it is different from retinal scanning. Automated high speed iris capturing and precision identification make iris identification systems the world's most advanced access and entry point security identification system (Patel, Trivedi and Patel, 2012, p. 4). The reason it is preferred is the iris has a unique pattern hitch that is formed by ten months of age and remains unchanged throughout one's lifetime. It is impossible for two irises to produce the same code. Iris recognition is non-contact and quick, and offers unmatched accuracy when compared to any other security alternative, from distances as far as 3" to 10" and only takes about 2 seconds ((Patel, Trivedi and Patel, 2012, p. 5).

Figure 15. Illustration of Iris Scan from istockphoto.com

4. Summary of Current Biometric Technologies (Modalities)

In a review of the literature, research and interviews with policy makers and trying to discover what would best enhance security in the RBS Aviation Passenger-Screening Program, a consensus was reached that the best modalities to be utilized are face, fingerprint and iris. DNA is highly unique and impossible to replicate, but difficult to obtain and thus is not used. As can be seen by the research, each of these modalities has its limitations and no single

biometric can bring about the desired performance universally, but the usage of multiple modalities is very promising. This leads to the suggestion that using not just one single modality, but the combination of more than one would provide the best theoretical solution to enhance aviation security.

E. ANALYSIS OF BIOMETRICALLY ENHANCED SECURITY SYSTEMS

1. DHS' United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program

The Department of Homeland Security established the U.S. Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program to collect, maintain, and share data on selected foreign nationals entering and exiting the United States at air, sea and land ports of entry (POE). These data, including biometric identifiers like digital fingerprints, are to be used to screen persons against watch lists, verify visitors' identities and record arrival and departure (Government Accountability Office, 2006,). The United States has more than 300 official ports of entry where nearly a half billion crossing occur every year. The Department of State (DOS) considers more than 9 million visa applications annually. DHS processes nearly 50,000 requests for asylum annually and processes approximately 30,000 applications for immigration benefits every day (National Science and Technology Council, 2008, p.28). In 2003, the U.S.-VISIT was created as part of a continuum of security measures that begins overseas and continues through a visitor's arrival in and departure from the United States. It incorporates eligibility determinations made by both the Departments of Homeland Security and State.

The U.S.-VISIT program works by visitors applying for a visa overseas at the visa-issuing post where each visitor has his or her biographic and biometric information – 10-point digital finger scans and a digital photograph – captured by a State Department official. Then, upon a visitor's arrival in the United States, U.S. CBP Officer uses an inkless digital finger scanner to electronically capture ten finger scans. The visitor is asked to put the left hand fingers and then the

right hand fingers on the scanner. The CBP Officer also takes a digital photograph of the visitor. The biographic and biometric data are used to match the visitor with the travel documents and is compared against watch lists. The CBP officer then proceeds with questions about the visitor's stay and then either admits the visitor or conducts additional queries based on the verification results. These procedures are designed to reduce fraud, identity theft, and the risk that terrorists and criminals would enter the United States undetected (www.globalsecurity.org/security/ops/usvisit.htm, 2012). Over the last 10 years, the U.S.-VISIT program has evolved into a biometric and biographic identity verification and watch list-matching service. The biometric information that is gathered is stored in DHS's Automated Biometric Identification Database (IDENT) and is shared throughout the Homeland Security community.

Analysis shows the U.S.-VISIT program provides biometric information and analysis services for the Department of Homeland Security agencies including, CBP, ICE, U.S. Border Patrol, U.S. Coast Guard and the Department of State. Through the use of biometrics the program greatly enhances immigration and border management, law enforcement and intelligence communities ability to accurately identify people and determine if they pose a risk to the United States. The U.S.-VISIT program can rapidly identify and verify U.S. visitors' identities to help verify the identities of legal and illegal individuals attempting to enter the United States. It has also been a great source for assisting the United States intelligence community with identifying KSTs and terrorist suspects (National Science and Technology Council, 2008, p.28–29).

Figure 16. Illustration of U.S. Visit Biometric Data Capture from CBP, 2012

2. TSA's Transportation Worker Identification Credential (TWIC) program

Within the Department of Homeland Security, the Transportation Security Administration and the U.S. Coast Guard manage the Transportation Worker Identification Credential (TWIC) program, which requires maritime workers to complete background checks and obtain a biometric identification card to gain unescorted access to secure areas of regulated maritime facilities (Government Accountability Office, 2011). TWIC was established by Congress in 2002 through the Maritime Transportation Security Act (MTSA) and is administered by the Transportation Security Administration (TSA) and the U.S. Coast Guard. The TWIC is a tamper-resistant biometric card that will be issued to workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities, and all credentialed merchant mariners. It is anticipated that more than one million workers (including longshoremen, truckers, port employees, and others) will be required to obtain a TWIC. The TWIC contains two biometric templates of a person's fingerprint. These templates are stored on the card in a format that is enciphered using a card-specific TWIC privacy key. To confirm a cardholder's identity and ensure it matches the stored biometrics, the data on the card are retrieved, deciphered, verified, and matched against a live finger. TWIC uses biometrics for two primary identification purposes: background screening

and verification. Background screening occurs prior to the issuance of a TWIC and encompasses an FBI criminal history records check and a check of DHS' IDENT database. Post-issuance, biometrics may be used at access control points to ensure that the biometrics of the individual attempting to use the TWIC match those stored within the credential (National Science and Technology Council, 2008, pp.33–34).

Analysis of the TWIC program shows that a TWIC is required for all unescorted access to individuals such as longshoremen, port operator employees, truck drivers and rail worker which allows them access to secure areas of port facilities, rail yards and vessels regulated under the Maritime Transportation Security Act. TWIC is a biometric identification card with a customized computer chip containing a biometric identifier of a ten-finger fingerprint, a 2D digital photograph template, biographic information, and digital certificates. This biographical data is utilized to authenticate a worker's immigration and work authorization status. Background checks are conducted including a review of criminal history records, terrorist watch lists, immigration status and outstanding warrants on the individual prior to being issued.

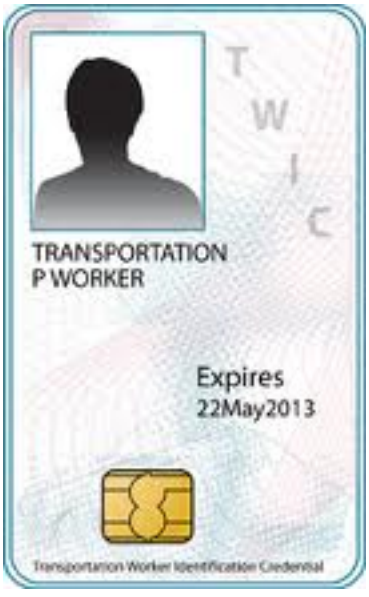

Figure 17. Illustration of TWIC Smart Card from TSA, 2012

3. CBP's Global Entry (GE) program

Global Entry is a program managed by U.S. Customs and Border Protection (CBP) that allows pre-approved, low-risk travelers expedited clearance upon arrival into the United States. The Global Entry program is the U.S. government's expedited border crossing program for individuals in the United States that are predetermined to be low risk, returning from international destinations. Upon returning from international travel, Global Entry-enrolled travelers may bypass the regular passport control line and proceed directly to the Global Entry kiosk. The Global Entry process will require participants to present their machine-readable U.S. passport, Global Entry card, or permanent residency card, submit their ten-point fingerprints, have a digital photo taken for biometric verification, and make a customs declaration at the kiosk's touch screen. The kiosk will compare the fingerprints presented to the fingerprints on file as well as compare the digital photo taken to the digital photo on file to confirm the traveler's identity. Upon successful completion of the Global Entry process at the kiosk, the traveler will be issued a transaction receipt and directed to baggage claim and the exit unless chosen for a selective or random secondary referral (National Science and Technology Council, 2008, p.36).

U.S. CBP officials and law enforcement agencies issue Global Entry cards to low risk travelers whose personal data has been subject to numerous background and security checks. Global Entry is open to U.S. citizens, lawful permanent residents, Dutch citizens, and Mexican nationals. Canadian citizens and residents may enjoy Global Entry benefits through membership in the NEXUS or SENTRI programs. U.S. Customs and Border Protection and law enforcement agencies run checks to determine if the individual has a criminal or immigration violation against him/her. These checks are repeated every time the traveler uses his/her Global Entry card. Any traveler with a criminal record or immigration violation will be automatically denied enrollment into the program. Recently, TSA has partnered with U.S. Customs and Border Protection as well as U.S. air carriers to incorporate a TSA program, TSA Pre✓™ that expedites

screening. TSA Pre✓™ utilizes the Global Entry program (including SENTRI and NEXUS) to determine eligibility for their expedited screening program.

Analysis of the Global Entry program shows that international entry into the United States is leveraging biometrics to expedite customs and immigration processes while adding increased scrutiny and security within the systems and protocols. Biometrics have automated entry into the United States, while verifying identities of individuals entering and has expedited the screening and traveling process. The TSA does not biometrically verify the individual's identity when utilizing the less scrutinized TSA Pre✓™ expedited screening lanes. There is only a verification of the traveler's elite status as a frequent traveler or possession of a Global Entry (SENTRI or NEXUS) card and no automated biometric check is performed.

Figure 18. Illustration of Global Entry Kiosk from CBP, 2012

4. Summary of Biometrically Enhanced Security Systems

Examination of the U.S. government biometrically enhanced security programs shows they have made tremendous strides in utilizing biometrics to identify and verify individuals' identity. These programs are focused on international passengers and international travel and provide identity verification

through fingerprints and facial recognition to allow entry into the United States by land, sea or air. A fundamental shortcoming of these programs is they have been designed individually and separately from each other and are proprietary to that particular program. They have recently begun sharing databases, but there has been no universality or standardization amongst the programs to gain synergy utilizing these biometrically enhanced programs. Analysis begs the question of why hasn't biometrically enhanced security been used for domestic travel? The next chapter leads into how to integrate biometrics into the domestic RBS Aviation Passenger-Screening Program.

V. FINDINGS AND RECOMMENDATION

A. FINDINGS

The central idea of this thesis is how to incorporate biometric technology / programs into the Risk-Based Security Aviation Passenger-Screening Program. The integration and synthesis of biometric technology into the domestic screening process would validate the passenger's identity, further increasing the security effectiveness and reliability of the passenger's identity. One of the fundamental issues that has arisen is passengers who have been classified as low risk and authorized to use the TSA Pre✓™ checkpoints have not had a thorough background check and do not meet all the requirements to utilize the lane. For example, a requirement to use TSA Pre✓™ is the traveler must be a U.S. Citizen with a clear police investigation background check, yet we are finding foreign nationals being granted access to these TSA Pre✓™ lanes. The reason being is the airline industry has given us our initial low-risk population through its high time frequent flyer members program. The vetting of these individuals has been less than ideal creating a larger security gap than previously existed.

1. RBS Initiative Programs Findings

Through research and analysis it was discovered that there is no standardization processes for the risk-based security initiatives for the Aviation Passenger Screening Program. In the analysis it was discovered there were no standardized enrollment processes to be considered for the pre-check program, KCM program or DoD CAC program. For enrollment into TSA Pre✓™, passengers could come from multiple areas: a member of the Global Entry program including SENTRI and Nexus; being a high time frequent flyer for one of the participating airlines; or possessing a DoD CAC for entry into the program. The enrollment process for becoming a member of Global Entry, for example, is one must go through a full background check, have biometric templates created

of both a 2D digital facial image and a ten-point fingerprint taken and stored in the DHS IDENT database, opt in voluntarily, and pay a fee. Additionally, the traveler is issued a biometric card that contains his/her 2D digital facial image, fingerprints and biographical data (note; biometric data and biographical data stored is not utilized for the verification of identity). In comparison, participating airlines nominate pre-check candidates from amongst their best customers and high time flyers who voluntarily opt in to receive the same privileges with no background check or surrendering of biometrics. Furthermore, it was discovered any Armed Forces service-members on active duty status or even currently discharged who still possess their DoD CAC card are eligible to enter into the TSA Pre✓™ lanes for reduced procedures and expedited passenger screening (note: biometric data and biographical data stored on the card is not utilized for verification of identity).

That KCM program that offers pilots and flight attendants to bypass all security screening procedures only uses personal documentation identity comparison. The pilot or flight attendant produces his/her airline credentials, which are then visually verified against a computer query of the airlines database (note; no biographical data or biometric data is stored on their credentials only a visual comparison is done). KCM is set up for fingerprint biometrics, but they are not utilized for identity verification. Additionally, the control and data entry into the database is controlled by the individual airlines. This creates a possible security vulnerability within the security system since the airlines are not part of the TSA and there are several databases that need to be queried (each airline has their own) leading to more access points for vulnerabilities within the system. With one database under the control of the TSA the risk and vulnerability would be reduced for the system and it would then become more efficient (Ryan, 2010, pp.1–4).

2. Current Biometric Technologies (modalities) Findings

This research found that each individual technology has limitation in universality, uniqueness, permanence, collectability, or performance,

acceptability, and/or circumvention. Due to these limitations, no single biometric can provide a desired performance and the usage of multimodal biometric traits is promising. Exploiting information from multiple biometric sources or features improves the performance and also robustness of person authentication (verification and/or authentication) (Hossain and Chetty, 2011, p.142). In analysis it was found the best biometric modalities to be utilized for authentication are facial, fingerprint and iris.

Facial recognition is among the different modalities used in biometrics, the face is considered to be the most transparent one. IT requires minimum cooperation from the subject. In some application scenarios, like crowd surveillance, face recognition probably is the only feasible modality to use. Face recognition is also the natural way used by human being in daily life (Li and Barreto, n.d. p.1). Facial recognition is one of the most acceptable, non-intrusive physiological attributes used to authenticate individuals. For face recognition, the performance of a 2D face matching systems depends on capability of being insensitive of critical factors such as facial expression, makeup and aging, but also relies upon extrinsic factors such as illumination difference camera viewpoint, and scene geometry (Hossain and Chetty, 2011, p. 142). Furthermore, even though 2D facial recognition has achieved considerable success, certain problems still exist because the 2D face images used not only depend on the face of a subject, but also depend on the imaging factors such as the environmental illumination and the orientation of the subject (Li and Barreto, n.d. p.1). The most promising right now is 3D facial recognition. There have been great developments in 3D imaging technology and facial recognition making it the better alternative in the field of biometrics. Unlike facial recognition using 2D images, 3D facial images capture the exact geometry of a person and it is invariant to illumination, environment and orientation of the person being authenticated.

Fingerprints are the most widely used system for authentication. The FBI has been using it for over a century and the current IAFIS system has over 70

million criminal fingerprints and 34 million civilian fingerprints in it. The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small-to-medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors aging, environmental, or occupational reasons (e.g., manual workers may have a larger number of cuts and bruises on their fingerprints that keep changing) (Jain, Ross and Prabhakar, 2004, p.9).

Iris recognition appears to be the best type of authentication process available today. Iris recognition is the most prominent biometric capture technique that can be implemented. To capture an image of the iris is very simple. Iris recognition takes a picture of the iris; this picture is used solely for authentication and is different from retinal scanning. An iris security system is a smoother, smarter and more secure identification system. Automated high-speed iris capturing and precision identification make an iris identification system the world's most advanced access and entry point security identification system. Using iris recognition technology has reduced errors to less that one in 1.2 million ensuring highly precise individual identification. Confusion or duplication with another individual is virtually impossible. No physical contact makes it perfectly safe. The individual merely needs to stand in front of the camera and a very weak amount of infrared illumination is used to capture the image.

Iris recognition is preferred because it is: Stable; the iris in humans has a unique pattern hitch and is formed by 10 months of age and remains unchanged throughout one's lifetime. Unique; it is impossible for two irises to produce the same template. Flexible; Iris recognition technology can be easily integrated into existing security systems. Reliable; Iris pattern is unique and not susceptible to theft, loss or compromise. Non-invasive; Iris recognition is quick, non-contact and offers unmatched accuracy when compared to any other security alternative from distances as far as 3" to 10" unlike retinal scanning (Patel, Trivedi and Patel, 2012, pp.4–5).

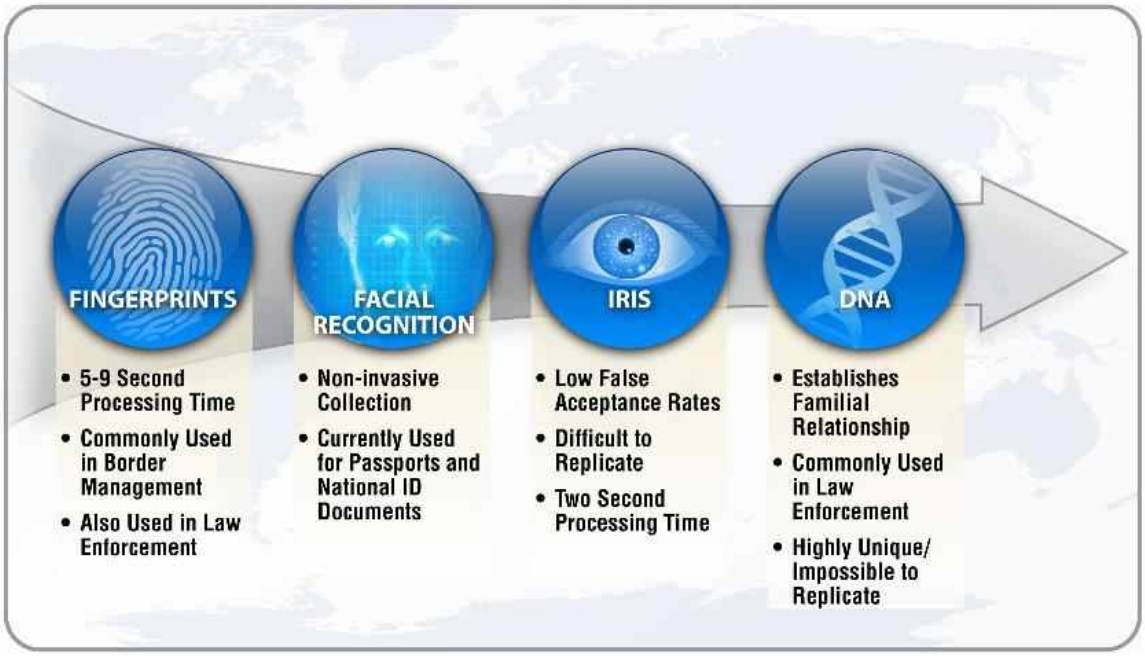

Figure 19. Advantages of Biometric traits from Le, 2011

3. Biometrically Enhanced Security Systems Findings

In analysis of DHS' United States Visitor and Immigrant Status Indicator Technology (U.S.-VISIT) program, it was found the program processes and maintains biographic and biometric information collected by other federal entities such as the State Department and U.S. Customs and Border Protection (CBP). U.S.-VISIT also shares information on the entry and departure of foreign visitors who pass through U.S. ports of entry. U.S.-VISIT processes biometric information

such as fingerprints and photographs that, along with other biographic and biometric information that it shares with other Federal entities,, can be used to verify foreign nationals' identities, authenticate travel documents, and determine the admissibility of visitors, immigrants and refugees (Office of Inspector General, 2012, p.2). The data collected is stored in IDENT. The U.S.-VISIT program checks the person's biometrics against a biometric watch list of more than 6.4 million known or suspected terrorists, criminals, and immigration violators identified by U.S. authorities and Interpol. When a foreign visitor presents an identification document, U.S.-VISIT can check the person's biometrics against other files that could be accessed to ensure that the document belongs to the person presenting it and not someone else (Office of Inspector General, 2012 p.3). More importantly, U.S.-VISIT functions both as an identification system and a verification system. In the case of identification, U.S.-VISIT serves as a negative identification system by utilizing watch list information, such as the Federal Bureau of Investigation's Criminal Master File, to identify individuals who should be denied entry into the United States and possibly apprehended or detained by law enforcement officials (GAO, 2008, p.55). In the case of verification, U.S.-VISIT is used to verify the identities of travelers who have been enrolled in the system. The program utilizes verification of individuals against databases such as the DHS IDENT and FBI IAFIS databases and [hopefully] in the future, DoD's ABIS (Biometrics Task Force, 2010, pp.1–2). The U.S.-VISIT program has also faced its challenges by having fraudulent biographic identities. In a recent inspection, 825,000 incidents were found where the same fingerprints were associated with different biographic data. Additionally, the program has struggled to deliver the exit portion of the program in the United States thereby not having a biometrically based capability for knowing the status of the foreign nationals who have entered our country.

In analysis of the Transportation Worker Identification Credential (TWIC) program, it was found that the program was designed to create a common credential for transportation workers across the United States who required

unescorted access to secure areas at the Maritime Transportation Security Act (MTSA) regulated maritime facilities and vessels. The TSA and USCG oversee this program jointly. The goal of the program is to positively verify the identification of authorized individuals (low-risk) access to secure areas of our nation's transportation system. Each individual had to go through a thorough security and background check to assess their level of security risk; low-risk, unknown risk and high-risk. Additionally, the individuals had to enter the program voluntarily and submit biometric data including fingerprints and digital photo. Their biographical and biometric data is then utilized for a background check against local and federal sources and is stored in the FBI's IAFIS database. Furthermore, their information is checked against federal terrorism information from the terrorist screening database including the selectee and no-fly list (GAO, 2011, pp.9–11). Upon successful background check a TWIC card is issued which is a smart card with a small integrated circuit chip that can be read by inserting it into a card slot in a "contact" card reader or holding within 10 centimeters of a "contactless" card reader. It also has a magnetic strip and a linear bar code. The card contains biometric data and biographical information. The card is valid for five years at an initial enrollment fee of $129.75. As of March 2012, the TWIC program has enrolled 2.1 million maritime workers and has issued almost 2 million credentials. The program has improved maritime security by using a federally issued and sponsored credential to enhance access control to secure areas at MTSA regulated facilities, vessels, and areas of our nation's transportation system. The program has not been without challenges, however. In a recent GAO report, it pointed to a lack of standardization in the enrollment process, which included an inability to provide reasonable assurance that only qualified individuals were enrolled. The system does not have a constant feedback loop to continually check the eligibility of TWIC cardholders. After enrollment the national databases are not checked again. This does not allow for verifying that a TWIC cardholder may have become ineligible after receiving his/her TWIC (GAO, 2012, pp.12–13).

In the analysis of the Global Entry program it was found that the Global Entry program in 2012 became a permanent Customs and Border Protection program that allows low-risk, pre-approved travelers expedited access into the United States from foreign travel. The program requires a very thorough and rigorous background check and interview process. Furthermore, it is a voluntary program where biographical information and biometric data is provided and stored in the DHS IDENT database. Additionally, a smart card is issued containing the biographic and biometric data of the individual. The way the traveler enters into the United States is through a Global Entry kiosk in lieu of waiting in long lines for border and customs clearance. The traveler merely presents his/her passport, permanent resident card or Global Entry card, provide fingerprints and digital photo for identity verification against the credential provided and then makes a customs declaration. If all the requirements of identity verification are met, a receipt is printed and the traveler proceeds to the exit. Note, they may be randomly selected for further examination or inspection at any time. As of mid-2012, there are kiosks in over 25 major airports across the United States that have been used over 6 million times, reducing traveler wait times by 70 percent and saving CBP officers more than 50,000 inspection hours, allowing them to focus resources on individuals of unknown or high-risk status (Zuckerman, 2012, pp.1–2).

In summary of these findings, the U.S.-VISIT program utilizes biometrics and biographical data and verifies them against national databases (IDENT, IAFIS and ABIS) to verify identity and threat assessment against the United States. The TSA/USCG TWIC program uses biographic and biometric data along with smart card technology to verify identity and allow individuals into the secure areas of our transportation system. The novel Global Entry program uses biographic and biometric data along with kiosks to expedite customs and immigration entry into the United States while verifying identity and threat assessment. This program also reduces resources and assets needed while increasing efficiency of customs clearance.

4. International Biometric Programs-Automated Border Clearance (ABC)

Since 1997, the international community has continually embraced and improved upon using biometrics to expedite passenger travel while reducing security resources and increasing security efficiency through the use of biometrics. A majority of Europe has adopted ABC systems to handle medium to high inbound or outbound traffic. ABC systems enable eligible and cleared passengers to gain permission to access Europe's national transportation system, which includes crossing national or regional borders by simply interfacing with ABC kiosks and gates. The gates use biometrics such as fingerprints or facial images to confirm the identity of the traveler while performing background checks simultaneously. These automatic biometric systems allow a way to expedite large volumes of travelers without the need for additional staffing and increase the efficiency and security of the entire national transportation system (Accenture, 2010). Many of these programs are single modal programs and have recently transitioned to multi-modal systems for travel, entry and border clearance. Some of the programs that have been successful are:

SmartGate Australia; an automated border clearance and processing program that allows eligible travelers with electronic passports to self-process through passport control. SmartGate is a two-step process. The first step, at the kiosk, is where the electronic passport is read and a ticket issued to the passenger. Step two, the gate, the passenger inserts the ticket and biometric verification matches the passenger's live photo with the reference image read from their electronic passport. SmartGate uses facial biometric technology. The reference image read from the electronic passport is biometrically compared with a live image of the passenger. An Australian survey found an 86 percent approval from the travelling public who found it easy to use and 99 percent would use it again (Frontex, 2010, pp.28–29). The system is said to cut the processing time from 45 to 17 seconds with a 98 percent success rate (Accenture, 2010).

Figure 20. Photo of SmartGate (Facial and Fingerprint) Brisbane International Airport from Frontex, 2010

The RAPID border control system was the first system to use biometrics in Europe. RAPID was first utilized in Portugal for border control for travelers using electronic passports and was a way for the government to control immigration and internal transportation security. The way it works is a photo of the passenger is taken at the automated gate and a live match is performed to the smart card or electronic passport with facial biometrics. After the identity is verified the automatic gate opens and the traveler is allowed to enter. Since 2007, RAPID has reduced the border control process to an average of less than 20 seconds per person resulting in processing 180 passengers per hour. An estimation of a reduction in human resources cost by approximately 55 percent has been forecast.

Figure 21. Photo of RAPID gates (Facial Recognition) at Faro Airport Portugal from Frontex, 2010

The Privium system in the Netherlands is a voluntary opt-in frequent flyer program for Europe. The program uses a smart card containing the traveler's biometric information. The biometric data that is stored is the iris template. The travelers entering or exiting the Netherlands are fast tracked into a separate border control line where kiosks accept the Privium smart card. Iris cameras are used to verify the traveler's identity against the smart card. This program has been highly successful in the Netherlands (Accenture, 2010).

Figure 22. Photo of Privium system in the Netherlands (Iris Scan) from Airport Business, 2009

The biometric e-Gate system, in the United Arab Emirates, has created a faster more efficient movement of passengers. It uses biographical data and biometric data. The new system quickly scans the electronic passport as well as acquires biometric data including facial and retinal scan. The system then matches the captures biometric information against databases and existing lists to detect potential threats. It is estimated that these new procedures are performed in 12–14 seconds while maintaining a high level of accuracy and security efficiency (The Gulf Today, 2012).

Figure 23. Photo of e-gate at Dubai Airport UAE (Facial and Retinal) from The Gulf Today, 2012

In summary, since 1997 until today, biometrics have been embraced by our international allies as a way to verification and identification of travelers and citizens. The progress made has led to multi-modal biometric systems that are now incorporating more than just one biometric trait. Most recently, the United Kingdom now utilizes face, iris and fingerprints. Spain now uses face and fingerprints. The Netherlands is now incorporating the face along with the iris and

Finland is incorporating the face with fingerprints as well. Biometrics has definitely come to the forefront for large scale identity authentication which in turn improves security, increases the flow of passengers and frees up human resources to be utilized elsewhere on higher risk passengers (Accenture, 2010).

Figure 24. Photo of new United Kingdom Border Control (Facial and Fingerprint) from ThirdFactor, 2012

B. RECOMMENDATION

The Transportation Security Administration should integrate a biometrically enhanced security system into the current RBS Aviation Passenger-Screening Program. Create a prototype of the ideal security checkpoint utilizing biometrics could be designed by collaborating with and integrating some of the best multi-modal biometric authentication systems available. In a review of the findings, biometrics incorporated into the current RBS initiative programs (TSA Pre✓™, DoD CAC and KCM) would be able to close security identity verification

gaps with passengers by simply adding a biometric system into the RBS APSP during the pre-check phase. The best way to incorporate this would be to have an automated biometric clearance station or kiosk at the front of all pre-check security lanes. The features of the biometric security station would include:

- Biometric identity cards or biometric passports to validate a person's identity prior to entering the TSA Pre✓™ line. The passenger enters with a biometric smart card, which would have the traveler's biometric template for facial, fingerprint and iris.
- While at the biometric security station, a picture is taken while simultaneously obtaining fingerprints and an iris scan. It would be a combination of a 2-dimentional biometric facial recognition along with an iris scan and failsafe five-finger fingerprint scan.
- The biometrics obtained at the security station are then compared to the templates stored on the smart card. Thee biometric information gained at a kiosk would then be cross-referenced against the information stored on the biometric card or passport and also the national biometric databases to give certainty and validity to the person's identity before they are allowed to enter.
- During authentication, if the identity of the traveler is verified, he/she is allowed to enter the pre-check lane for expedited security screening. The information gathered would be sent to the Triad of biometric Databases (DoD's ABIS, FBI's IAFIS {NGI} and DHS IDENT), which would validate the identity and also search for any illicit activities or warrants tied to the traveler.
- After expedited security screening the traveler then enters into the national transportation system.

Besides being utilized for identity verification (1:1), it can also be used for identification authentication (1:n) if the biometric information gathered is sent to one of the national databases for verification. If the system can be integrated with the national databases, this would also become a powerful law enforcement tool. This would have the added benefit of assisting law enforcement agencies in identifying known suspects and people of interest. This would be an incremental innovation after being tested on our low-risk passengers, we could offer it to our

normal risk passengers on a volunteer basis, and eventually, offer it to high-risk passengers.

Collaborating with Customs and Border Protection's Global Entry program could yield extensive benefits by adopting the Global Entry program's structure and system. This new TSA biometric program could utilize the already established CBP Global Entry network by making modifications to meet the needs of domestic travelers and entering into the national transportation system. The kiosk could be modified to include iris scanning. The TSA could issue a biometric smart card, much like the TWIC. All participants could voluntarily opt-in for expedited convenience with a fee to cover the maintenance fees and cost of the program. Additionally, the biometric records could be stored in a national database, preferably the FBI IAFIS and soon to be NGI. The control of all stored biometric data would be in control of the U.S. government instead of private corporations such as CLEAR which had fiscal difficulties and bankruptcy.

Furthermore, the process for enrollment should be standardized to allow for consistent background checks and vetting of individuals unlike the programs now that allow high time frequent flyers to be eligible to enroll without background checks. The Global Entry program and the new TSA domestic travel program utilizing a standard card that is valid for both international as well as domestic entry into the national transportation system. This could create a significant cost savings and resource reduction for both the CBP and the TSA.

Finally, this standardized system could be utilized for KCM. This would allow for a standard enrollment with background checks done by the U.S. Government. The KCM databases would then be integrated into the national databases and provide quality assurance over the identification of the pilots and flight attendants. Furthermore, it would incorporate and identity verification step at the security station or kiosk and eliminate manual matching done by the Transportation Security Officers. The system could be fully automated which would further eliminate costs and resources needed for entry into the national transportation system.

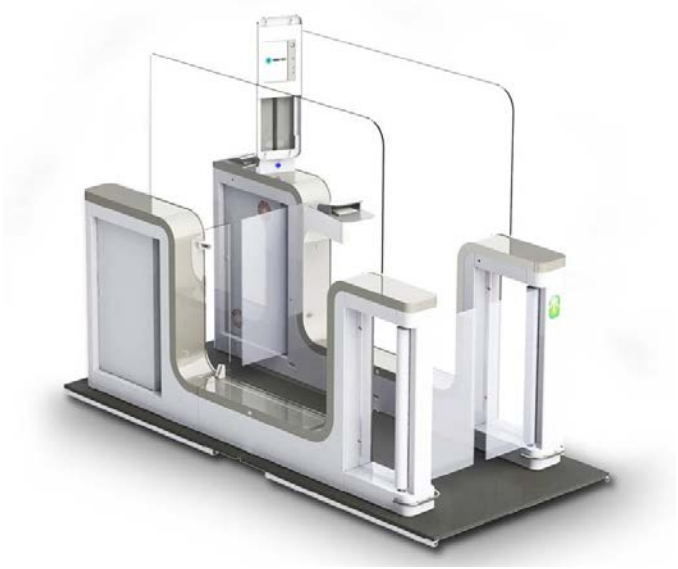

Figure 25. Illustration of future checkpoint (Facial, Fingerprint and Iris) from Visio-Box, Copyright 2012

Figure 26. Photo of e-Passport gates at Terminal 4 in London's Heathrow Airport (Facial, Fingerprint and Iris), from Accenture, 2012

VI. CONCLUSIONS

A. DISCUSSION OF THE RESEARCH

1. Biometric Security Systems

Biometric security systems are a new technology, but there are many applications and solutions for the use of biometric technology to exponentially enhance security systems. The main purpose of the biometric security system is to verify and identify a person's identity. This biometric technology is the most convenient over other protection technologies of identity authentication. For example, driver's licenses and ID cards that are used to authenticate a user's identity. In the current RBS Aviation Passenger-Screening Program, an attempt is made to check the authenticity of the travel document presented ensuring that it is not fraudulent, instead of trying to authenticate a person's identity we are not utilizing identification (1:n) or verification (1:1) processes to know who the person really is.

There are many advantages to using biometric security systems. First and foremost is the uniqueness of biometric technology. Each individual's identification will be the single most effective identification for that user. A chance of two users having the same identification in the biometric security technology system is nearly zero (Le, 2011). It is also extremely hard or impossible to make duplicate or shared biometric accessing data with other users and is less prone for users to share access to highly sensitive data since they have to use biometrics. This makes the system even more secure allowing user information and data to be kept highly secure from unauthorized users. Lastly, the identification of users cannot be lost, stolen or forgotten since it is the person's biometric that allows them access to the system. Most biometric security systems are easy to install and have become fairly inexpensive.

Some of the disadvantages of biometric security systems are each biometric modality has a weakness, which may cause some problems with the

interface with the biometric security system. For example, fingerprints could be problematic if the individual loses his/her fingers or does not have fingers at all. For iris or retinal scanning biometric systems, psychologically users find it very intrusive and have concern for the safety of their eyesight. Databases used to store user identification will be very large and require new and modern technology so initial startup may be expensive for the equipment required for the storage and security of the data (Le, 2012).

2. Strategic Benefits

The utilization of biometric stations or kiosks would verify the biometric identity (1:1) of passengers carrying smart cards or electronic passports, it could reduce the number Travel Document Checker's (TDC) stations and the time required to validate passenger documentation. At the station or kiosk, the traveler's identity would be validated and his/her airline gate pass would be endorsed to allow them into their proper security checkpoint, would be accomplished in one location. Furthermore, it could reduce the number of Transportation Security Officers required by eliminating the majority of the Travel Document Checker stations with this new station or kiosk while simultaneously increasing the scrutiny of the traveler, making for a better overall aviation passenger security screening process and lessening the risk for validation of identities. Reducing the number of TDC stations in turn reduces the number of human assets required and thus reduces budgetary costs. The efficiency and effectiveness of the checkpoints would increase because of reduced inspection requirements and the burden of removing shoes, jackets, laptops etc. Wait times would lessen because of the improved procedure and lines would decrease by validating trustworthy passengers who would need fewer inspections and scrutiny at security checkpoints since they are a low risk or threat to the aviation enterprise. This new approach greatly increases risk mitigation from the current approach we have today. In the future the biometric station or kiosk can be used for identification authentication (1:n). This new system would allow the ability to cross-reference numerous government databases with biometric data to

authenticate the identification of the traveling passenger presenting his/her biometrics. A secondary function would be to cross-reference any other illicit activities the traveler may be associated with such as outstanding warrants. The overall benefits would be increased security efficiency through verification or identification of traveling passengers. This would reduce the number of manning and budgetary requirements while increasing the speed of processing and reducing the wait times as well as increasing the capacity of the screening lanes, which improves the entire traveling experience.

B. IMPLEMENTATION CHALLENGES

1. Oppositional Agendas to the Incorporation of Biometrics

The main opposition to the incorporation of biometrics into the Aviation Passenger-Screening Program would be civil liberties groups, union and personal privacy and trust issues. The main opposition to biometrics and the gathering of biometrics is that it is a violation of our civil liberties. The American Civil Liberties Union (ACLU) has been the largest voice on this. It contends that after the biometric information has been collected and stored in one of the Triad databases, specifically the FBI's Next Generation Identification (NGI), the FBI would then tie-in computers to this biometric database and link them to surveillance cameras throughout the United States. They fear it would be a step toward mass surveillance of the population, which poses a "grave danger" to American values. They suggest it is more than just invasive; it is a fundamental revolution of American values. Additionally, there are many conspiracy theorists who prescribe to the Orwellian 1984 theory that "Big Brother is watching you" or Aldous Huxley's "*Brave New World*" where genetics and biometrics are utilized to determine one's class in life. Another opponent that may arise by incorporating biometrics is the American Federation of Government Employees (AFGE). They could arbitrate to not have biometric kiosks installed because it might eliminate government positions. This would decrease the U.S. Government's largest unionized workforce. The AFGE would want to maintain the status quo or grow to

improve their political power and lobbying efforts. Furthermore, there are personal privacy issues such as the right to be left alone. Privacy is generally viewed as a selective disclosure of personal information founded on the equilibrium between one's private life and his/her accepted social identity. One of the first major challenges with privacy is that biometrics are not like a password or token that can be revoked once they have been presented. Individuals are concerned that by using biometrics systems, they leave behind a trail of information that is very personal in nature and can reveal very personal information about them such as retinal scans can reveal images regarding certain medical conditions. Another privacy challenge for biometrics systems is the user's inability to control the collection and uses of the biometric information. This presents an important question for travelers; do travelers need to provide consent before biometric information is collected and utilized and can this biometric information be sold to third parties for marketing purposes. In order to establish privacy for the biometric system, information collected must only be used for the purpose for which it was collected. The information must be stored on a device owned by the user, smart card or biometric passport. The individual must be educated on the rights of the biometric system user. This shows the traveler's sense of privacy influences the adoption of biometric systems for travel. The last challenge is trust. The traveler must trust in the organization to whom he/she is providing biometric information. Travelers' sense of trust associated with biometric systems greatly influences the adoption of the biometric system and travel (Morosan, 2012, pp.187–188).

2. Allies and Agendas

There are far more allies than opponents in the biometric incremental innovation to change this complex adaptive system. As stated earlier, the TSA is looking for efficiency and speed at the checkpoints, which leads to more revenue and a better travel experience. Some of these allies and agendas are the Air Line Pilot's Association, International (ALPA), Airlines for America (A4A) and the International Air Transport Association (IATA) as well as, all the commercial

airlines. These organizations want to reduce requirements of the screening process while increasing the throughput and speed of the Aviation Passenger-Screening checkpoints. The agenda is, the more efficient and faster a checkpoint is, the more flights they can book and the more revenue that is generated. The airline associations' agenda is clear; profit. The TSA has assisted with this by standing up Known Crew Member (KCM). To illustrate, the ALPA and A4A in conjunction with the TSA, entered into a joint, collaborative checkpoint security procedure with airline pilots. The way the KCM program works is, the airline pilot, with his credentials, enters a special checkpoint that has no walk through metal detector or X-ray machine, just a biometrically enhanced card and fingerprint reader attached to a computer. After presenting credentials, the computer then validates the credentials against a database and allows the airline pilot and crew to pass without having to endure any of the screening processes. This process only takes a matter of seconds versus minutes, which further reduces the congestion at the other checkpoints. All these organizations endorse this program because it maximizes the crew duty day by reducing the amount of time spent at checkpoint screening. It has been estimated that 30 minutes to an hour out of their duty day has been gained by not standing in screening checkpoint lines. Yet another agenda might come from the large scale specialized manufacturers of screening equipment such as L3 and Rapid Scan. Utilization of biometrics would improve the efficiency of checkpoints without the necessity of current technologically enhanced screening equipment, thus reducing walk-through metal detectors, X-ray machines and Advanced Imaging Technology (body scanners) sold and utilized by the U.S. government throughout the 460 federalized airports. Lastly, the more clandestine agendas would be the FBI wanting access to the current, live streaming biometric data presented at the checkpoints. They would want to track people of interest and Known Suspected Terrorists (KST). This would allow them to easily locate suspects quickly and covertly. Many agendas would be served or disadvantaged with the incorporation of biometrics depending on the organization.

3. Wild Cards

The budgetary cost of the TSA to the U.S. taxpayer has been ballooning at a time when we are looking for ways to be more fiscally responsible. At the same time, air travel has been expanding. The TSA's budget from 2004–2010, increased by over 68% while the number of air travelers remained relatively the same. In the near future our fiscal constraints and government cutbacks may require a large reduction in the federalized workforce or force the return to commercialization of aviation passenger screening, much like the model at San Francisco International Airport where passenger screening is done by contractors. If U.S. budgetary constraints on the horizon are what they are expected to be, the TSA could cease to exist as an agency and our technologically enhanced security measures including biometric identity validation could also cease to exist based on lack of available funding.

In 2010, there were 263 million air travelers in the United States. The FAA predicts that by 2021 that number will increase to 1 billion U.S. air travelers per year. Another possible wild card would be that air travel becomes too costly for the upper middle class or below to travel. The airline industry revenues would then constrict and there would no longer be a requirement for screening that is done today. Airline travel would only be available to the very wealthy and/or private aircraft owners. If the airline industry as we know it collapsed, there would be no requirement for the screening we have today.

After 9/11, the Aviation Passenger-Screening Program was initially a disruptive innovation. The entire screening process was upended and revamped, involving federalizing the work force to include 60,000 Transportation Security Officers (TSO's). Technology was introduced to detect prohibited items (i.e., knives, guns, etc.) along with introducing government regulations to control and standardize aviation passenger screening checkpoints. This was a fundamental departure from the way passenger screening had been done in the past when the airlines controlled the screening process. There was no standardization and very little security value. Since 2002, we have been on an incremental innovation

approach to passenger screening. With every threat that has occurred, we have introduced technology to overcome the issue. For example, the 2009 underwear bomber led us to introduce the new Advanced Imaging Technology (AIT), otherwise known as the body scanner. All this accomplished was adding billions of dollars to screening and increasing the number of screening requirements and inspections done to passengers which in turn led to longer lines and longer wait times at checkpoints.

The Aviation Passenger-Screening Program has continued to be an adaptive system since its inception, but it has been unsuccessful in adapting properly to the environment in which it was designed to benefit; the airline industry. It has almost had the opposite effect and become a burden by driving up costs, increasing wait times, slowing passenger flow and increasing the hassle of air travel which lessens the number of flights people take. In reality, this has not increased security significantly but has given the appearance that it has. We have mastered finding prohibited objects going on airplanes; however, we are still quite naïve when it comes to finding bad people, with ill intent, who wish to do us harm and preventing them from boarding planes.

In late 2011, the Transportation Security Administration introduced changes to this complex adaptive system; called Risk Based Security (RBS) initiatives. RBS is a process that classifies passengers into different risk categories based on information gained during a pre-screening passenger risk assessment. This risk assessment then aligns security protocols to their pre-screening risk assessment. Now we have what is called the TSA Pre✓™ checkpoint where passengers who have received a low-risk pre-screening are allowed to go to the TSA Pre✓™ checkpoint, keep their shoes and jacket on, as well as, keep their liquids and laptops in their bags. This has greatly increased the efficiency and speed of the checkpoint while reducing wait times and passenger travel hassles.

C. FUTURE RESEARCH

This thesis is very narrowly crafted to just review the current biometric modalities that are out there to current biometrically enhanced security programs that can be utilized to improve our current Risk-Based Security Aviation Passenger Security Program. The goal was to help create an ideal model where biometrics could be utilized to enhance risk based security using biometrics. Due to the limitations and scope of this thesis, these final results could not be all inclusive or a totally encompassing solution to improve Aviation Passenger Screening. There are other areas of research.

1. 3D Facial Recognition

Future research can be looked at utilizing 3D facial recognition in place of the 2D facial recognition currently being used. In lieu of using 2D recognition, 3D facial recognition greatly enhances the efficiency and accuracy of using facial recognition as biometric identification and verification method. 3D facial recognition holds great promise. 3D modeling enhances recognition performance because it can be used to recognize people in profile versus a typical forward-looking “mug shot” pose. This could lead to scanning people while waiting in security checkpoint lanes for screening. They could even walk through the cordoned area where they could be recognized and allowed to go directly to RBS APSP. Research would have to be conducted to determine how 3D facial recognition could be integrated.

2. TSA Biometric Data Sharing and Integration With Other Federal Agencies

Future research can be done on the collection of biometric data through the TSA’s biometrically enhanced checkpoint. These biometric stations/kiosks could be utilized by integrating the world’s two largest biometric databases, the FBI’s IAFIS and DHS’ IDENT. Each database holds over a hundred million records. If the databases could be integrated for interoperability and data sharing we could have a very powerful biometric database for identification (1:n) and

verification (1:1). A study would have to be conducted to research how the databases could be integrated into the RBS APSP.

3. Biometrics and Privacy Concerns

For many years now the public has had concerns about the gathering of biometrics; more specifically, gathering biometrics for facial recognition. If this new system could gather 2D or 3D photos to identify a person in a public place, one would no longer have anonymity in a public place. A simple comparison of a photo of an individual to one of the biometric databases would reveal the identity and biometric data of that individual. This in turn raises the privacy concern some individuals may have. The privacy concern may be the most troublesome issue that will have to be addressed. Is the public willing to sacrifice some of their liberty for the sake of their safety and security? As Benjamin Franklin stated, “They that can give up essential liberty to obtain a little temporary safety deserve neither safety nor liberty.”

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Accenture. “Accenture helps BAA and the UK Border Agency to automate Heathrow border clearance and achieve high performance.” Accenture: High performance. Delivered. Chicago, IL: Accenture, 2011.

Accenture. “Insights into Automated Border Clearance.” Accenture: High performance. Delivered. Chicago, IL: Accenture, 2010.

Accenture. “The business of biometrics: How integrated biometrics can help public service organizations achieve better business outcomes.” Accenture: High performance. Delivered. Chicago, IL: Accenture, 2011.

Airport Business. Airport Security & Safety. www.airport-business.com/2009/10/promoting-a-single-eu-border-control-standard (accessed October 13, 2012).

AlMahafzah, Harbi and AlRwashdeh, Ma’en. “A Survey of Multibiometric Systems.” International Journal of Computer Applications 43, no. 15 (April 2012): 36–39.

Bartlow, Nick and Zekster, Gregory. “Holistic Evaluation of Multi-Biometric Systems.” BRTRC, October 2009.

BIMA. Annual Report FY11. Annual Report, Biometrics Identity Management Agency, Washington: BIMA, 2011.

Biometrics Task Force. The Biometrics Triad: Working to seamlessly Integrate Biometric Data. January 2010. www.biometrics.dod.mil/Newsletter/issues/2010/Jan/v6issue1_a4.html (accessed May 22, 2012).

Center for Army Lessons Learned (CALL). Commander’s Guide to Biometrics in Afghanistan. Vols. 11–25. For Leavenworth, KS: CALL, 2011.

Crosby, Mark. “Taking Risk Based Security to the Next Level.” Airport Magazine, August/September 2012.

Defense Manpower Data Center (DMDC)/Identity Services (IS). FAQ-Users. www.dmdc.osd.mil/smartcard/owa/ShowPage?p=faqusers (accessed October 12, 2012).

Elias, Bart. Airport Passenger Screening: Background and Issues for Congress. Report to Congress, Congressional Rese, Washington: Congressional Research Service, 2009.

FBI. Fingerprints & Other Biometrics. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2 (accessed May 22, 2012).

—. Integrated Automated Fingerprint Identification System. www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (accessed May 22, 2012).

Federal Aviation Administration. FAA Aerospace Forecast. Forecast, U.S. Department of Transportation, Federal Aviation Administration, Washington: FAA, 2012.

Frontex. Biopass II: Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate. European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, Rondo: Frontex, 2010.

Global Security . Homeland Security: United States Visitor and Immigrant Status Indicator Technology (U.S. VISIT). www.globalsecurity.org/security/ops/usvisit.htm (accessed October 13, 2012).

Government Accountability Office. Border Sercurity: U.S.-VISIT Program Faces Strategic, Operational, and Technological Challenges at Land Ports of Entry. Report to Congressional Requesters, GAO, Washington: GAO, 2006.

Government Accountability Office. Strategic Solution for U.S.-VISIT Program Needs to Be Better Defined, Justified, and Coordinated. Report to House of Representatives, Homeland Security, Government Accountability Office, Washington: GAO, 2008.

Government Accountability Office. Transportation Security Administration: Progress and Challenges Face in Strengthening Three Key Security Programs. Testimony, Washington: GAO, 2012.

Government Accountability Office. Transportation Worker Identification Credential: Internal Control Weaknesses Need to Be Corrected to Help Achieve Security Objectives. Report to Congressional Requesters, GAO, Washington: GAO, 2011.

Hicklin, Austin, Ulery, Brad, Watson, Craig. A Brief Introduction to Biometric Fusion. Study, Department of the Interior, National Institute of Standards and Technology, Washington: NIST, 2006.

Homeland Security Defense Business Council. “The 9/10/11 Project.” Government Security News, May 10, 2011.

Hossain, S.M.E. and Chetty, G. “Next Generation Identity Verification Based on Face-Gait Biometrics.” International Conference on Biomedical Engineering and Technology. Singapore: IACSIT Press, 2011.

Jackson, Brian A., Chan, Edward W., LaTourrette, Tom. Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. RAND Research Report, RAND, Arlington: RAND Corporation, 2011.

Jain, Anil K., Ross, Arun and Prabhakar, Salil. “An Introduction to Biometric Recognition.” IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics 14, no. 1 (January 2004): 1–28.

Kumar, V.K. Narendira and Srinivasan, B. “New Biometric Approaches for Improved Person Identification Using Facial Detection.” I.J. Image, Graphics and Signal Processing (Modern Education and Computer Science (MECS) Press) 8 (August 2012): 43–49.

Le, Chien. “A Survey of Biometric Security Systems.” 2011.

Li, Chao and Barreto, Armando. Biometric Recognition of 3D Faces and Expression. Electrical & Computer Engineering Department, Florida International University, Miami: Florida International University.

Li, Chao and Barreto, Armando. “Profile-Based 3D Face Registration and Recognition.” Computer Science 3506, no. 73–104 (2005).

Lynch, Jennifer. From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond. Special, Immigration Policy Center, Washington: American Immigration Council, 2012.

Morosan, Christian. “Biometric solutions for today’s travel security problems.” Journal of Hospitality and Tourism Technology 3, no. 3 (2012): 176–195.

National Research Council of the National Academies. Biometric Recognition Challenges and Opportunities. Research Report, Engineering and Physical Sciences, National Academy of Sciences, Washington: National Academy of Sciences, 2010.

National Science and Technology Council. Biometrics in Government Post 9/11. Report, Biometrics and Identity Management, National Science and Technology Council, Washington: NSTC, 2008.

National Science and Technology Council. The National Biometrics Challenge. Report, Subcommittee on Biometrics and Identity Management, National Science and Technology Council, Washington: National Science and Technology Council, 2011.

Office of Inspector General. Letter Report: U.S.-VISIT Faces Challenges in Identifying and Reporting Multiple Biographic Identities. Letter Report, Office of Inspector General, Department of Homeland Security, Washington: DHS, 2012.

O'Toole, Alice J., Phillips, P. Jonathan, Jiang, Fang et al. "Face Recognition Algorithms Surpass Humans." TSWG, 2006.

Patel, Chandrakant D., Trivedi, Sanket and Pate, Sanjay. "Biometrics in Iris Technology: A Survey." International Journal of Scientific and Research Publications 2, no. 1 (January 2012): 3–4.

Peterman, David Randall, Elias, Bart, Frittelli. Transportation Security: Issues for the 112th Congress. Report to Congress, Congressional Research Service, Washington: Congressional Research Service, 2011.

Podio, Fernando L. and Dunn, Jeffrey S. "Biometric Authentication Technology: From the Movies to Your Desktop." ITL Bulletin, May 2001: 1–8.

Poole, Jr., Robert W. "Airport Security: Time For a New Model." Policy Study 340. Los Angeles, CA: Reason Foundation, January 2006.

Riley, K. Jack. "Air Passenger Security at a Reasonable Cost." Edited by John Godges. Rand Review (RAND Corporation) 35, no. 2 (Summer 2011).

—. "Air Travel Security since 9/11." RAND, 2011.

Riley, K. Jack. "Flight of Fancy? Air Passenger Security since 9/11." The Long Shadow of 9/11: America's Response to Terrorism (RAND), 2011.

Ross, Arun A., Nandakumar, Karthik, Jain, Anil K. Handbook of Multibiometrics. New York, New York: Springer, 2006.

Ross, Arun. "An Introduction to Multibiometrics." 15th European Signal Processing Conference (EUSIPCO). Morgantown: West Virginia University, 2007.

Ryan, Tim. "ARINC 2G CrewPASS Architecture: Biometric Stand-Alone System." ARINC. Baltimore, MD: ARINC, November 2, 2010.

The Gulf Today. Novel smart e-gate at Dubai airport to usher in new era of passenger service. 2012. http://gulftoday.ae/portal/3e402648–2906–499b-92e5–58e5765194d0.aspx (accessed October 28, 2012).

The White House. “Biometrics for Identification and Screening to Enhance National Security.” National Security Presidential Directive and Homeland Security Presidential Directive. Washington, DC, June 5, 2008.

ThirdFactor. UK’s Stansted Airport deploys biometric e-passport gates. www.thirdfactor.com/2010/01/26/uks-stansted-airport-deploys-biometric-e-passport-gates (accessed October 13, 2012)

Transportation Security Administration. “Expedited Passenger Screening Pilots.” Washington, DC: Transportation Security Administration, August 2011.

—. “Moving TSA to a High Performing Organization.” TSA’s Counter-Terrorism Strategy. Washington, DC: Transportation Security Administration.

—. “Risk-Based Security.” TSA Vision. no. 45. Washington, DC: U.S. Department of Homeland Security, June 22, 2012.

—. Secure Flight Program. October 12, 2012. www.tsa.gov/stakeholders/secure-flight-program (accessed October 15, 2012).

—. What We Do. 2012. www.tsa.gov/what_we_do/rbs.shtm (accessed May 10, 2012).

—. What We Do/How it Works. 2012. www.tsa.gov/what_we_do/howitworks.shtm (accessed May 10, 2012).

U.S. Department of Homeland Security. “Automated Biometric Identification System (IDENT).” Privacy Impact Assessment. Washington, DC: Department of Homeland Security, July 31, 2006.

—. Government Agencies Using U.S.-VISIT. March 4, 2011. www.dhs.gov/files/programs/gc_1214422497220.shtm (accessed May 22, 2012).

—. Learn about TWIC. 2011. twicprogram.tsa.dhs.gov/TWICWebApp/AboutTWIC.do (accessed May 22, 2012).

—. Statement of John S. Pistole, Administrator, Transportation Security Administration... June 2, 2011. www.dhs.gov/ynews/testimony/testimony/13069054825846.shtm (accessed 2011).

—. Written testimony of Transportation Security Administration Administrator John Pistole for a Senate Appropriations, Subcommittee on Homeland Security Hearing titled “Balancing Prosperity and Security: Challenges for U.S. Air Travel in a 21st Century Global Economy. April 2, 2012. www.dhs.gov/news/2012/04/02/written-testimony-transportation-security-administration-administrator-john-pistole (accessed September 10, 2012).

U.S. House of Representatives. A Decade Later: A Call for TSA Reform. Joint Majority Staff Report, U.S. House of Representatives, 112th Congress, Washington: 112th Congress, 2011.

U.S. House of Representatives. Rebuilding TSA into a Smarter, Leaner Organization. Majority Staff Report, 112th Congress, Washington: U.S. House of Representatives, 2012.

U.S. Travel Association. “A Better Way: Building a World Class System for Aviation Security.” Washington, DC: U.S. Travel Association.

Whither Biometrics Committee. Biometric Recognition: Challenges and Opportunities. Engineering and Physical Sciences, National Research Council of the National Academies, Washington: The National Academies Press, 2010.

Yager, Jordy. TSA head wants ‘risk-based,’ tailor-made airport screening. February 10, 2011. thehill.com/news-by-subject/defense-homeland-security/143357-tsa-head-wants-risk... (accessed July 27, 2011).

Zuckerman, Jessica. Global Entry Reciprocity: Creating a Trusted Traveler Superhighway. Brief, Center for Foreign Policy Studies, The Heritage Foundation, Washington: The Heritage Foundation, 2012.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. John Pistole
   Transportation Security Administration
   Arlington, VA

4. John Halinski
   Transportation Security Administration
   Arlington, VA

5. Chris McLaughlin
   Transportation Security Administration
   Arlington, VA